PERFORMANCE ANALYSIS OF INDUSTRIAL MULTI-HOP WIRELESS SENSOR NETWORK IN OIL AND GAS INDUSTRY

BY

ABDULLAH MOHAMMED AL-YAMI

A Thesis Presented to the

DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

ELECTRICAL ENGINEERING

JANUARY 2017

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

This thesis, written by **ABDULLAH MOHAMMAD AL-YAMI** under the direction of his thesis adviser and approved by his thesis committee, has been presented to and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN ELECTRICAL ENGINEERING (EE)**.

Thesis Committee

Dr. Wajih Abu-Al-Saud (Adviser)

Dr. Wessam Mesbah (Member)

Dr. Khurram Karim Qureshi (Member)

Dr. Ali Al-Shaikhi
Department Chairman

Dr. Salam A. Zummo
Dean of Graduate Studies

1/6/17
Date

This work is dedicated to my beloved Mother

ACKNOWLEDGMENTS

In the name of Allah, the Most Gracious, the Most Merciful.

All Praises are due to Allah Lord and Sustainer of the universe. Peace and blessings of Allah be upon our noble Prophet Muhammad, his family and his Companions.

I would like to acknowledge the support and opportunity provided by the department of Electrical Engineering and Deanship of Scientific Research at King Fahd University of Petroleum and Minerals (KFUPM).

I am thankful to my advisor, Dr. Wajih Abu-Al-Saud, for his guidance, help, and support during this research. I am grateful to him for his great sense of care, respect and flexibility to me in my research and academic work. Many thanks are also due to my thesis committee members Dr. Wessam Mesbah and Dr. Khurram Karim Qureshi for spending their valuable time and providing useful comments and feedbacks towards the successful completion of my work.

Finally, I would like to thank all friends and colleagues who helped me in any capacity during my stay at KFUPM.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

THESIS ABSTRACT

NAME: Abdullah Mohammad Al-Yami

TITLE OF STUDY: Performance Analysis of Industrial Multi-hop Wireless Sensor Networks in Oil and Gas Industry

MAJOR FIELD: Electrical Engineering (EE)

DATE OF DEGREE: January 2017

Wireless automation is an emerging field of research that aims at achieving significant savings in installation time and costs of cabling in automation systems, while providing a new level of flexibility for system design, reconfiguration, and agility. Despite the advantages of wireless networks, there are many phenomena that promptly degrade the performance of wireless systems. Fading is one of the major contributing factors that degrade the wireless service, and environment is a major source of fading. The fading effect could be short term or long term. In order to curb this factor, techniques such as the use of multi-hop communications and high data rate modulation schemes such as QPSK, 8-PSK and 16-PSK have gained popularity in the field of wireless communication. This thesis research simulates diversity techniques using channel fading models such as Rayleigh fading, Nakagami fading and Rician fading over co-operative wireless sensor networks and proposes the best channel modulation scheme. A proposed error correction

diversity scheme is also simulated and compared with some standard diversity techniques. Further, to access the performance of WSNs in industrial settings, simulations and experiments are carried out for ISA100.11a, Zigbee and WirelessHart. In the experiments the actual Packet Error Rate (PER) and Received Signal Strength Indicator (RSSI) values are gathered in different scenarios.

CHAPTER 1

INTRODUCTION

Wireless Sensors are small and portable devices that are used to sense and transmit relatively small amounts of data required parameters from a remote location. Wireless sensors have proven their importance in wide range of fields such as industries, oil and gas sector, environmental research and defense sector. They are used to monitor the temperature, humidity, pressure and other environmental factors. Since they are randomly deployed and are densely populated, many topologies like star or mesh are used to collect the data in efficient manner. In the past, industries used sensors that were wired to a central station. The major disadvantage of this deployment is the need for huge infrastructure, high installation and maintenance cost and non-scalability of the system. Wireless networks are an obvious replacement since these are scalable, have low cost, are mobile, are self-organizing and are easy to maintain and deploy. However, security and integrity of the system is an issue that needs to be addressed [1].

1.1 Motivation

Industrial Wireless Sensor Networks (IWSNs) have played a significant role in industrial automation since the time of its introduction. IWSNs do not only improve the efficiency of an industrial system but also reduce threats to life and equipment by generating and delivering real time instrument parameters in harsh operating environments. Cost reduction and scalability are additional advantages of IWSNs. Even with their myriad merits, IWSNs are prone to challenges such as high memory and power requirements when operating in such harsh environments. Addressing these challenges will not only improve battery life of the IWSNs which is critical for their operation but will also improve their operation reliability as compared to wired industrial sensor networks. Several wireless protocols have been developed to address these challenges. Key among them are Zigbee, ISA100 and WirelessHart, which are designed to deal with challenges inherent in wireless sensor networks [1]. The main aim of this work is to simulate these protocols and discuss their pros and cons. A practically calculated and simulated parameters comparison is also planned that will help us understand the factors that affect communication networks in the real world. The idea behind the simulation is to visualize the output of the system before implementing it practically. Simulations represent the key to understanding the step by step operation of any system. Different network scenarios can be developed and simulated on the wireless protocols' specific platform so as to estimate the behavior of the network in different environments. Also it is not possible to check the system functionalities in worst case scenarios or disasters, e.g. it is really very difficult to estimate

the network breaking point in case of heavy rain, hail and wind but this could be easily characterized in simulation. There is always a little difference between practical and simulated values which is mainly due to the factors which are not considered in the simulation but are present and play their part in real environment. The smaller the difference the better the estimation of the environment, hence one aim of this work is to calculate the difference between simulation of IWSNs and practical experimentation.

1.2 Research Objectives

The thesis objectives can be summarized as follows:

1. Conduct a comprehensive literature survey on the the existing methods and challenges in adapting WSN for industrial applications:
    - Review of three commonly employed WSN protocols in industrial environment.
    - Background study of diversity techniques and channel fading and evaluate the performance of the error correction technique for co-operative WSNs.
2. Perform field experiments of IWSN protocols and analyze the results.
3. Simulate IWSN protocols in various deployment scenarios.

1.3 Expected Outcomes

- A Study about the feasibility and challenges of utilizing IWSN.

- Comparison of three protocols i.e. Zigbee, WirelessHart and ISA 100 in terms of throughput, communication cost per node and energy consumption.
- Study of Diversity techniques and channel fading.
- Comprehensive simulation and validation using Castalia and Pymote.
- Documentations and publications involving all the skills and expertise that have been gained during this research.

1.4 Organization of the Thesis

The rest of this thesis is organized as follows. Chapter 2 provides a comprehensive review of the literature regarding IWSN systems and diversity techniques. Diversity techniques and channel fading concepts and simulations are discussed in Chapter 3. In Chapter 4, the experimental results of simulation of IWSN protocols are analyzed. Comprehensive simulation and validation of IWSN protocols using Castalia and Pymote are presented and analyzed in Chapter 5. Finally, Chapter 6 concludes the thesis with the list of contributions/publications of this research and proposes some future directions.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Wireless Sensor Networks (WSN) [1][2] are small sensors that are deployed in remote locations to sense particular conditions and send information pertaining to these conditions to a Central Control Room (CCR). WSN are ad hoc in nature and their number is often large. They work with limited resources and are irreplaceable. WSN have endless applications; it can be used in defense to monitor borders. They are also used by environmentalists to monitor environmental changes such as temperature and humidity in certain regions. For industries, WSNs can sense temperature and/or pressure of certain devices. WSNs have certain limitations such as low range, small battery size, and network structures which require a very resource efficient algorithm. Industrial Wireless Sensor Network (IWSN) evolved from WSN and are specially designed keeping in mind the demands and nature of industry [3].

IWSNs use bigger and high rating batteries and generally have wider transmission

range as compared to traditional WSNs. IWSNs have an edge over traditional wired structures since they can be installed easily anywhere in industry without heavy support structures. IWSNs can also work efficiently where wired networks are technically not installable such as on moving or rotating objects. Another important industrial requirement is the stability of the system. The system should be stable and easy to handle and maintain [4]. Also, deployed networks should be reliable and secure with high data rate support. Many protocols are developed that support the above functionalities. Zigbee is a wireless open global standard which satisfies the unique needs of low power, low cost and wireless machine-to-machine (M2M) networking. It is also used in IWSNs [5]. Zigbee is standardized by Zigbee alliance which consists of more than 300 companies. It can support star, mesh and tree topologies [12][18].

Another developed protocol is Highway Addressable Remote Transducer Protocol commonly known as WirelessHART and approved by International Electrotechnical Commission (IEC). WirelessHART is simple, secure, reliable, and uses TDMA with mesh topology. HART, like OSI model, uses many layers that add to security, integrity and reliability of the system [6].

ISA100, designed by International Society of Automation, supports high data rates up to 250 Kbps. Security and Integrity is provided by layered architecture. 6LoWPAN (an acronym of IPv6 over Low power Wireless Personal Area Networks), used in network layer, provides efficient routing and also enables IWSN to co-exist with other IWSN protocols. At the level of Physical Layer, IEEE 802.1.5.4 is used which uses Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) [10][14]. ISA works on 2.4

GHz free band with 16 channels. Transmitter complexity is significantly decreased by using Orthogonal Quadrature Phase Shift Keying (O-QPSK), which avoids the zero state and thus has a constant envelope transmission [12][23]. ISA100 uses the following layers to optimize performance:

1. A graphical user interface at its application layer.

2. For fast and reliable data transfer, User Datagram Protocol (UDP) is used at the transport layer.

3. At the network layer, IPv6 over Low power Wireless Personal Area Network (6LoWPAN) which can work with other networks.

4. At the data link layer, variable slot scheme is used.

5. IEEE 802.15.4 is used at the physical layer which is spectrally efficient and minimizes collisions between the adjacent nodes.

IWSN protocols usually use two types of devices to send data to CCR.

1. Field devices whose prime function is to sense the data and transmit it.

2. Gateway devices are responsible for receiving data and providing reliable transmission to CCR. Field devices can also reroute the packet to gateway devices. Far end devices usually transfer data over more than one hop.

2.2 Industrial Wireless Sensor Networks (IWSNs)

Wireless sensor networks are used mostly in commercial applications where the data requirement is not high [6]. But for industries, IWSNs are developed uniquely for industrial applications that can support high data rates, have high battery performance and can work in real time environments under high temperature and pressures. In industries, the conditions are usually tough. For this reason, sensors are developed in such a way to achieve high performance with minimum amount of errors [11]. The network architecture of IWSNs are mainly composed of three classes of devices as shown in Fig. 2.1.

1. Wireless End Devices (WEDs): these are the devices whose prime function is to sense the data and forward the information.

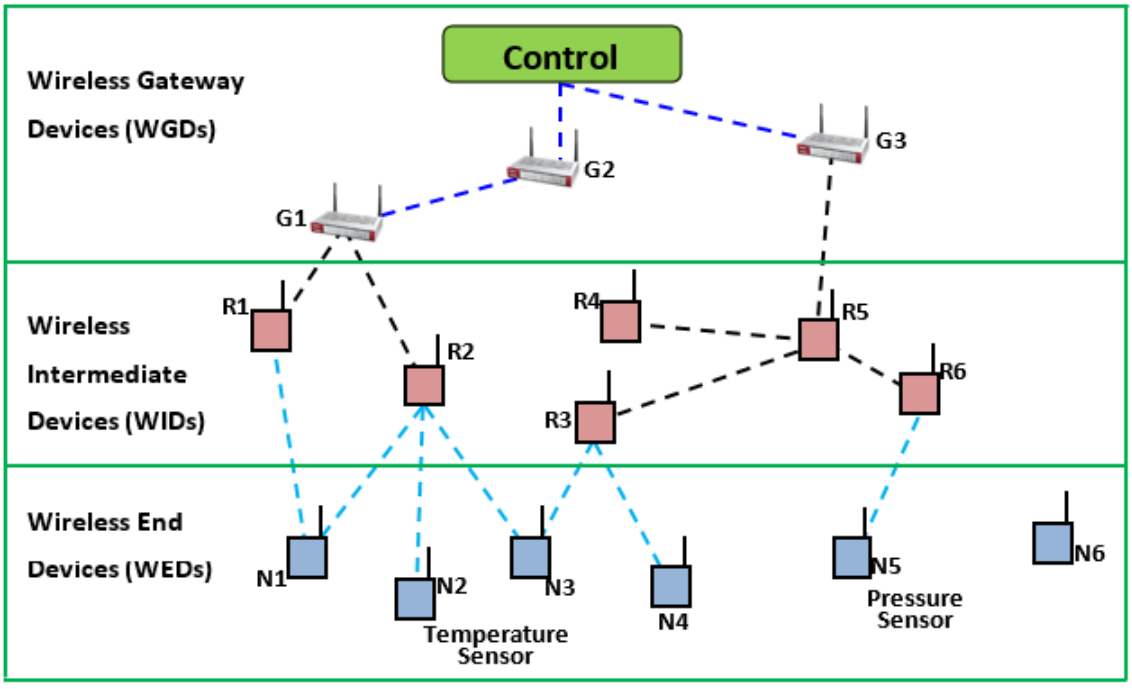


Figure 2.1: Architecture of IWSNs

2. Wireless Intermediate Devices (WIDs): these devices are intermediate devices that are used to sense as well as route the incoming data.

3. Wireless Gateway Devices (WGDS): these devices are used to gather data from incoming devices and forward to central station.

For wireless sensors, IEEE 802.11 standard defines the law for mobility and scalability. Different flavors of this standard also add to high data rates and secure transmission. Wireless networks usually work on 2.4 GHz band. Star and mesh topologies can be used based on the requirement of the industry. Usually redundant links are used to avoid single point of failures [10]. Despite all the developments and advantages WSNs have many drawbacks that need to be addressed.

- Wireless networks are degraded very much by the fading caused by the different elements that are present in the environment. Fading weakens the incoming signal and increases error rate in communication.

- Noise is another factor that affects the communication channel. It is commonly referred to as white Gaussian noise which cannot be avoided. A solution to the noise problem is to increase the transmission power at transmitter end. However, the power cannot be increased beyond a certain level since it reduces battery life.

- The received signal strength is also inversely proportional to the square distance between the transmitter and receiver. The higher the distance is, the lower the received signal strength at receiver will be. This is referred to as path loss. Low

received signal strength can be combated by increasing transmission power and using relays in systems.

- Also in specific environments there may exist multiple frequencies that introduce interference and noise. As a result, communication interferences are introduced. Multiplexing techniques are available that reduce these effects.

IWSNs face a lot of challenges in their implementation and operation. The properties of a wireless channel make it very difficult to determine the capacity of a wireless link. The delay incurred in the wireless channels is highly undesirable in real time applications such as for industrial process automation applications. The motivation behind this work is to study the performance of a customized model of an industrial wireless sensor network that proposes amendments on current communications protocols to make them suitable for oil and gas industry environments.

The main advantages of wireless networks are as below [12]:

1. Cost efficient
2. Suitable for emerging applications
3. High flexibility
4. High adaptability
5. High reliability

Wireless sensor networks (WSNs) are a rather new technology, with their origins tracing back to the early 1980s through the Distributed Sensor Networks (DSNs) program at

the Defense Advanced Research Project Agency (DARPA) of the US Department of Defense [1]. DSNs were imagined to consist of many spatially distributed, autonomous and low-cost sensing nodes that collaborate to gather information about their surroundings. However, in the 1980s, the technology was not quite ready for this application. Sensors were too large and expensive and communications were not yet associated with wireless connectivity.

In the late 1990s, advances in computing, communication and micro-electromechanical technologies caused a shift in DSN research, bringing it closer to achieving the original vision. The "second wave" of DSN activities started in 1998, and it attracted large international involvement and attention. New networking techniques and networked information processing suitable for the dynamic ad-hoc environments found in sensor networks were the initial focus, with the goal of enabling the required complex applications to run on resource-constrained sensors [1]. The sensors themselves have also evolved with new technology, reducing both their cost and size. In addition, advances in wireless technology enabled robust and reliable wireless communications ideally suited for wireless distributed sensor networks. DARPA was again the pioneer, leading the efforts of sensor network research. They initiated a research program which provided new insights into ad-hoc networking, dynamic querying and tasking, reprogramming and multi-tasking [1]. At the same time, IEEE started to note the potential of WSNs, and worked on a specification for low-rate wireless personal area networks [2].

The work of IEEE was finalized in 2003, when the IEEE 802.15.4 specification [2] was ratified, defining the physical layer (PHY) and medium access control layer (MAC)

for Low-Rate Wireless Personal Area Networks (LR-WPAN). The higher layers of the protocol stack were out of scope of the specification. Offering features such as low power, low complexity and low cost, it was ideally suited for WSN applications. With a growing number of solutions based on the IEEE 802.15.4 appearing in the years since its release, it has become the widely accepted standard for WSNs. The ZigBee specification [3], originally released in 2004, was the first full standard to appear based on the IEEE 802.15.4. ZigBee defines the Network Layer and Application Layer on top of the IEEE 802.15.4 PHY and MAC.

Early research and evaluation of the IEEE 802.15.4 identified several potential issues related to information security, in addition to other minor bugs and errors. A new version of the standard was released in 2006: IEEE 802.15.4-2006 [4], which addressed these shortcomings. The original standard from 2003 is referred to as IEEE 802.15.4-2003, to distinguish the two versions. Shortly after the ratification of IEEE 802.15.4-2006, the ZigBee Alliance released a new version of the ZigBee standard, ZigBee-2006 [5]. The original ZigBee standard is referred to as ZigBee-2004. ZigBee-2006 included improvements for, among other things, addressing issues leading to scalability problems for large networks. However, it is important to note that ZigBee-2006 was still based on IEEE 802.15.4-2003, and not on the new IEEE 802.15.4-2006. Hence the security issues of IEEE 802.15.4-2003 were still present in ZigBee-2006. In 2007, the HART Communication Foundation (HCF) released the HART Field Communication Protocol Specification, Revision 7.0 [6], which included a definition of a wireless interface to field devices, referred to as WirelessHART. WirelessHART was the first specification to be released which was specifically

designed for process automation applications. With features such as self-healing and self-configuring multihop mesh networks, WirelessHART offers a viable wireless alternative for the traditionally wired industrial field instrumentation. WirelessHART was approved by the International Electrotechnical Commission (IEC) as international standard IEC 62591 Ed. 1.0 for wireless communication in process automation [7] in March 2010.

The ZigBee specification was initially designed to address applications within home automation and consumer electronics. A ZigBee network operates on the same, user defined channel throughout its entire lifetime. This makes it susceptible both to interference from other networks operating on the same frequency and to noise from electrical equipment and machinery in the environment. As a result, ZigBee has not been regarded as robust enough for harsh industrial environments [8]. To combat this challenge, the ZigBee Alliance released the ZigBee PRO specification [9] in 2007. ZigBee PRO is specifically aimed at the industrial market, having enhanced security features and a frequency agility concept where the entire network may change its operating channel when faced with large amounts of noise and/or interference. Despite these innovations, ZigBee has not yet been fully adopted by the industry.

Parallel to HCF's work on WirelessHART, the International Society of Automation (ISA) initiated work on a family of standards for wireless systems for industrial automation applications. This resulted in the ratification of the ISA100.11a standard in September 2009 [10]. Like WirelessHART, ISA100.11a aims to provide secure and reliable wireless communication for non-critical monitoring and control applications in the process automation industries. A new version of the ISA100.11a was released in 2011

[11], addressing minor faults and errors in the initial specification.

A fourth specification addressing wireless communication for the process automation industries, WIA-PA, was accepted by the IEC in 2009 as IEC 62601 [12]. WIA-PA was developed by the Chinese Industrial Wireless Alliance (CIWA) under the urgent requirements of process automation. In 2007, CIWA was established by Shenyang Institute of Automation, along with more than 10 universities, academies, and companies. The scope of WIA-PA is to provide a system architecture and protocol stack for use in industrial monitoring, measurement and control applications. However, at the time of writing this work, no products supporting WIA-PA were readily available on the market.

In April 2012, the IEEE 802.15.4e [13] was released as an amendment to the IEEE 802.15.4 specification. It provides additional MAC behaviour and frame formats which allow IEEE 802.15.4 devices to support industrial applications such as process control and factory automation. No devices supporting IEEE 802.15.4e had yet been released, at the time of writing this thesis.

2.3 IWSN Communication Protocols

When discussing WSN specifications and solutions, it is helpful to understand the structure of communication protocol stacks. A protocol stack defines a set of layers, where each layer is a collection of related functions. A layer offers services to the layer above it, and uses services from the layer below. The most common communication stack model is the seven-layered OSI-Model. For WSNs, a simplified version of the OSI model is used, where the Presentation Layer and the Session Layer are not defined [12]. Note that not

all WSN standards define the Transport Layer either.

2.3.1 IEEE 802.15.4

The IEEE 802.15.4 [2] was initially released in 2003 and updated in 2006. The standard comprises four different physical layers (PHYs), three in the 868/915 MHz band and one in the 2.4 GHz band. A total of 27 channels are defined, numbered from 0-26. Channel 0 is in the 868 MHz band, Channels 1-10 are in the 915 MHz band and channels 11-26 are in the 2.4 GHz band. In the 2.4 GHz band the channel width is 5 MHz and the channel spacing is 2 MHz. As the 868 MHz (Europe) and 915 MHz (US) bands have limited geographical availability due to various national rules and regulations, most industrial applications uses the globally available 2.4 GHz band.

2.3.2 ZigBee / ZigBee PRO / ZigBee IP

The ZigBee specification [5], initially released in 2004 and updated in 2006 and 2007, is a low rate, low power WSN standard developed by the ZigBee Alliance. The specification defines network and application layers on top of the PHY and MAC layers of the IEEE 802.15.4-2003, and it is primarily targeting smart grid, home automation and consumer electronics applications. Since the ZigBee specification uses the PHY and MAC layers of the IEEE 802.15.4, they have the same modulation techniques, bandwidth and channel configurations.

A ZigBee network operates on the same, user defined channel throughout its entire lifetime. This makes it susceptible both to interference from other networks operating

on the same frequency and to noise from other sources in the environment. As a result, ZigBee has not been regarded as robust enough for harsh industrial environments [7]. To combat this challenge, the ZigBee Alliance released the ZigBee PRO specification [9] in 2007 in the shape of what is defined as another feature set. ZigBee PRO is specifically aimed at the industrial market, having enhanced security features and a frequency agility concept where the entire network may change its operating channel when faced with large amounts of noise and/or interference. Despite these innovations, ZigBee has not yet been fully adopted by the industry. The ZigBee Alliance announced in April 2009 that it will incorporate standards from the Internet Engineering Task Force (IETF) into future ZigBee releases, thereby opening up for IP-based communication in ZigBee networks. Of special interest for the ZigBee Alliance is the 6loWPAN working group which has created a Request for Comments (RFC4944) investigating the transmission of IPv6 packets over IEEE 802.15.4 networks. This work resulted in the ratification of the ZigBee IP specification in February 2013 [18].

2.3.3 WirelessHART

WirelessHART is a part of the HART Field Communication Specification, Revision 7.0 [6], which was ratified in September 2007. WirelessHART enables wireless transmission of HART messages, and was the first standard to be released which specifically targets industrial applications. WirelessHART was approved as IEC standard 62591 in 2010. WirelessHART is based on the IEEE 802.15.4 PHY and MAC, although the MAC has been modified to allow for frequency hopping. Furthermore, WirelessHART only operates

in the 2.4 GHz band, which allows for global availability. TDMA with frequency hopping is used as channel access method, and with a full mesh network topology, WirelessHART offers self-configuring and self-healing multi-hop communication.

2.3.4 ISA100.11a

The ISA100 standards committee of ISA aims to deliver a family of standards for wireless systems for industrial automation. ISA100.11a [11] was the first standard to emerge, being ratified in 2009 and updated in 2011. ISA100.11a is designed for secure and reliable wireless communication for non-critical monitoring and control applications. Critical applications are planned to be addressed in later releases of the standard. ISA100.11a is based on the IEEE 802.15.4 PHY and MAC, but the MAC has been adopted to allow for frequency hopping and extended security mechanisms. ISA100.11a only defines operation in the 2.4 GHz band. TDMA with frequency hopping is used as the channel access mechanism. ISA100.11a supports both routing and non-routing devices, so network topologies can be either star, star-mesh or full mesh depending on the configuration and capabilities of the devices in the network. An ISA100.11a network is able to carry multiple fieldbus protocols, such as Foundation Fieldbus, PROFIBUS and HART. There is also integrated support for IPv6 traffic and routing in the network layer.

2.3.5 Comparison Between WirelessHART and ISA100.11a

In most IWSNs, WirelessHART and ISA100.11a are preferred for communication ahead of Zigbee protocol. Zigbee is normally employed for smaller nodes used for small scale

applications. Although WirelessHART and ISA100.11a have many more similarities than differences, there are still some key technical properties that are different in the two standards. In the following sections, a breakdown of some of the most prominent features that separate WirelessHART and ISA100.11a are presented [8].

2.3.5.1 Flexibility

WirelessHART and ISA100.11a are inherently different regarding the operational flexibility and configuration possibilities that the specifications allow for. WirelessHART is a rather "simple" specification with very few optional or configurable parameters. ISA100.11a on the other hand, is a complex and comprehensive specification with many configurable and optional parameters found in different stack layers. These features are both strengths and weaknesses depending on the specific needs and requirements of the target applications and usage scenarios space.The strict and limited approach of WirelessHART ensures that practically all WirelessHART devices will have identical behavior, regardless of design and implementation choices made by the equipment providers. This should easily facilitate interoperability between multiple vendors, as all products adhering to the standard should be equal. This naturally comes at the cost of a lack of possibility to adapt and tailor the device and network behavior to specific application requirements. The wide range of available optional and configurable parameters in ISA100.11a allows for great flexibility for adapting network behavior to various application requirements. However, it may lead to interoperability issues if different vendors choose to implement different features of the standard. To combat this, ISA100.11a must define application profiles. A profile is a cross-layer specification that defines which options are mandatory

in the different protocol layers. Although profile definitions help with possible interoperability issues, it still requires extensive compliance testing and verification to achieve full vendor flexibility.

2.3.5.2 Protocol Support

WirelessHART is a wireless extension of the wired HART Field Communication Protocol Specification, and is naturally confined to using the command-based HART protocol for message exchange. All information and data in a WirelessHART network must be transmitted in the shape of HART Commands. The ISA100.11a application layer is object oriented, and implements tunneling features that allow devices to encapsulate foreign protocols and transport them through the network. Although successful tunneling of protocols depends upon how well ISA100.11a meets the technical requirements of the foreign protocol, it still opens up the possibility of transferring a multitude of wired protocols over an ISA100.11a network.

2.3.5.3 Coexistence

Since WirelessHART and ISA100.11a operates in the popular 2.4 GHz band, they are likely to be subjected to interference from other wireless networks operating in the same frequency band. In recent years, IEEE 802.11-based infrastructure has become commonplace in many process plants and facilities, and it is expected that most wireless instrumentation deployments will share the frequency spectrum with IEEE 802.11-based access points and mobile devices. Practical experiments have shown that the performance of IEEE Std. 802.15.4-based networks will be degraded when coexisting with IEEE 802.11

networks [21], and since WirelessHART and ISA100.11a inherits their physical layer from IEEE Std. 802.15.4, they will be subjected to such interference as well.

To mitigate the effects of interference, wireless protocols may employ various coexistence mechanisms. In WirelessHART and ISA100.11a, clear channel assessment (CCA) and channel blacklisting are the weapons of choice to combat the degrading influence from other wireless networks. However, the two standards have chosen to implement the two features in slightly different ways. WirelessHART employs manual channel blacklisting, where a network operator must manually configure which channels are available and which channels are blocked. ISA100.11a has an adaptive blacklisting mechanism, where each device in a network may autonomously blacklist channels which suffer from noise and/or interference. Furthermore, ISA100.11a defines four different CCA modes, where modes 1-3 are defined by IEEE Std. 802.15.4:

1. Energy Above Threshold: CCA reports a busy medium upon detecting any energy above a configurable threshold.

2. Carrier Sense Only: CCA reports a busy medium if a signal compliant with IEEE Std. 802.15.4 PHY modulation and spreading characteristics is detected.

3. Carrier Sense with Energy Above Threshold: CCA reports a busy medium using a logical AND/OR combination of Modes 1 and 2.

WirelessHART on the other hand, has fixed its CCA mechanism to mode 2.

With the correct configuration, ISA100.11a should be somewhat better equipped to handle coexistence with IEEE 802.11 networks. While WirelessHART only listen to

activity from other IEEE Std. 802.15.4 networks, ISA100.11a will by employing either CCA modes 1 or 3 to report a busy medium if any energy above a threshold is detected. If there is activity from a nearby IEEE 802.11 access point or client, the ISA100.11a device will back off and delay its transmission to the next available timeslot. This will naturally result in increased latency, but no power is wasted trying to transmit a message that will most likely not be received correctly by the destination device. In addition, the adaptive channel blacklisting mechanism of ISA100.11a can dynamically remove this problem completely by not using channels which show high IEEE 802.11 activity.

2.3.5.4 Quality of Service

Although Quality of Service (QoS) is a term with various meanings and interpretations depending on the context, it can here be accepted as a measure of the service quality that a network offers to applications and/or users [22]. With QoS comes the ability to control the resource sharing of a network by giving different priorities to various applications and data packets depending on their requirements. Higher performance levels can then be provided to specific applications and data packets through a set of measureable service parameters such as latency, jitter, packet loss, reliability and availability [23]. Support for QoS in wired networks is generally obtained by over-provisioning and/or traffic engineering [22]. With over-provisioning, extra resources are added to the network so that it is able to provide satisfactory services to all applications. As all users are served at the same service class, over-provisioning may become unpredictable during peak traffic. For resource-constrained WSNs, over-provisioning is not an ideal QoS method as the network often does not have the capacity to provide the required resources. In traffic engineering,

users and applications are assigned a different priority through a set of defined service classes. This method is also called service differentiation, and it is a widely adopted scheme for both wired and wireless networks to provide QoS guarantees [23]. For traditional wired computer networks there are two main models for service differentiation; integrated services (IntServ) [24] and differentiated services (DiffServ) [25]. The IntServ model maintains service on a per-flow basis, while the DiffServ model maintains service on a per-packet basis. For the packet-based nature of WSNs, DiffServ is the best suited mechanism for service differentiation [26]. In the DiffServ model, the source devices know the criticality of the data packets it is sending, and this criticality is translated into predefined priority levels. Other devices in the network also select the appropriate service level for data packets based on their priority. WirelessHART defines four different priority levels on the DLL [6]:

- Command (highest priority). The Command priority is used for packets containing network-related diagnostics, configuration or control information.
- Process Data. Packets containing either process data or network statistics shall be classified as Process Data priority. Only the control of the network is more important than the delivery of sensor data measurements from field transmitters or set-point information to actuators.
- Normal. If a Data Link Protocol Data Unit (DLPDU) does not meet the criteria for any of the other three priority levels (Command, Process Data or Alarm), it shall be classified with Normal priority.
- Alarm (lowest priority). Packets containing only network alarm and network event

information shall have a priority of Alarm.

These priority levels are primarily used for flow control and to mitigate potential network congestion points in the event of either a process upset or noise/interference deteriorating the RF channel(s). With the above mentioned mechanisms, network management packets have full priority while propagating through the network, allowing the network manager to keep the network operational. Network-induced alarms have a restricted flow through the network, ensuring that alarm floods do not disrupt or hinder the network operation. All other network traffic flows through the network as bandwidth and internal buffer spaces on the devices allow. Unfortunately there is only one priority level reserved for process data, which means that all sensors and/or actuators in a WirelessHART network share the same priority level, regardless of the requirements and criticality of the application they are serving. ISA100.11a uses contracts to define the setup and requirement of communication between two devices in a network. A contract is an agreement between the system manger and a device in the network that involves the allocation of network resources by the system manager to support the communication requirements of the device. All contracts are unidirectional, and they are established by the system manager upon reception of a contract request. ISA100.11a supports two priority levels: contract priority and message priority. The contract priority is the base priority for all messages sent using a specific contract. Four contract priorities are supported [11]:

- Network control (highest priority): May be used for critical management of the network by the system manager.

- Real time buffer: May be used for periodic communications in which the message

buffer is overwritten whenever a newer message is generated.

- Real time sequential: May be used for applications such as voice or video that need sequential delivery of messages.

- Best effort queued (lowest priority): May be used for client-server communications.

The message priority establishes priority within a contract using two messages priorities: high and low. The contract priority is specified by the application, during contract establishment time, in its contract request. It may be used by the system manager to establish preferred routes for high priority contracts and for load balancing the network. The combined contract and message priority is used to resolve contention for scarce resources when these messages are forwarded through the network.

2.3.5.5 Security

Both WirelessHART and ISA100.11a rely on a centralized security manager for the authentication of new devices, and the generation and management of security keys throughout the lifetime of the network. This means that the loss of the security manager will cause the loss of security mechanisms in the network. New releases of WirelessHART and ISA100.11a networks are combating this issue by offering redundant network and security manager solutions with automatic and transparent handover from the primary to the secondary system in case of failure.

In WirelessHART, all security features are mandatory, while ISA100.11a defines many security mechanisms as optional. Considering that security algorithms require additional processing time, memory, and power, making them mandatory means that devices that

may not require strict security policies cannot disable them to achieve benefits such as extended battery life. On the other hand, the ISA100.11a concept of having optional security features may be a security threat in itself, and also an issue when it comes to interoperability. Vendors might not choose to implement the full security suite, and different vendors might choose to implement different parts of the optional security features.

2.3.5.6 Suitability for safety applications

In safety applications, reliability and timeliness are the main requirements for the communication between sensors and the safety system. As opposed to control-loops, rapid update rates are normally not required, but safety communication must have mechanisms which ensure that data packets arrive within a specific deadline. For most safety systems, a query-based data delivery model is used where the safety controller periodically requests data from the sensors. Safety systems in the process industries are subject to comply with a certain Safety Integrity Levels (SIL). The standard IEC 61508 [27] defines SIL from a set of requirements that both accomplish hardware safety integrity and system safety integrity. There are four SIL levels (1-4), where SIL 4 is defined as the most dependable and SIL 1 as the least. Neither WirelessHART nor ISA100.11a directly supports the necessary certified SIL safety mechanisms as an integrated part of their specifications. A workaround for this is to use an already established and certified end-to-end communication protocol, such as PROFIsafe [28], which is designed to be implemented on top of the PROFINet fieldbus [29]. The recent development of the world's first wireless hydrocarbon gas detection system has proven that it is possible to achieve SIL2 end-to-end communication between a safety controller and a wireless sensor

by tunnelling PROFIsafe over ISA100.11a [30]. For WirelessHART on the other hand, limitations in currently available HART commands at the application layer, makes it impossible to implement the tunnelling mechanisms needed for full PROFIsafe support. PROFIsafe over WirelessHART will thus not be available before a potential modification and new release of the HART Field Communication Protocol Specification is available.

2.4 Communication over Fading Channels

In practice, channel fading is usually not flat, communication is affected mainly by multi-path environment. There are different kinds of fading coefficient distributions which exist between the sender and receiver, e.g Rayleigh, Rician, Nakagami distribution, etc. There could be more than one level of noise induced between the source and the base station depending on the surrounding. Also in the real world communication model digital modulation schemes such as BPSK, QPSK, n-QAM are used which significantly increase the data rate but also make the transmission SNR dependent. Depending on the multipath fading environment there are multiple copies received at the base station with different noise levels. One could avoid retransmission just by simply taking the best from all the received copies. Diversity combining techniques help the station to eliminate errors from the received transmission.

2.4.1 Channel Fading

Despite the advantages of wireless networks, there are many phenomena that promptly degrade the performance of wireless systems. Fading is one of the major contributing

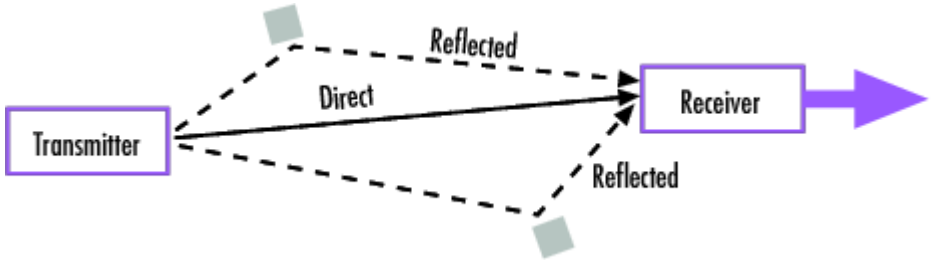


Figure 2.2: Wireless signal transmission

factors that degrade quality and strength of wireless signals. As shown in Figure 2.2,the fading is caused by multipath environment since the wireless signal like light could be affected by physical phenomenona like

1. Reflection
2. Refraction
3. Shadowing
4. Doppler effects

Fading causes bit errors, reduces the signal strength and can cause burst errors. As a result, the incoming packets may not be understandable by the receiver and hence needing retransmissions. Retransmission not only causes delay but also requires additional bandwidth. Reducing retransmission results in achieving higher data rates. The effect of fading is different for different frequencies.

Fading can affect radio communications channels in two main ways.

2.4.1.1 Flat fading

This form of multipath fading affects all the frequencies across a given channel either equally or almost equally. When flat multipath fading is experienced, the signal will just

change in amplitude, rising and falling over a period of time, or with movement from one position to another [1].

2.4.1.2 Frequency selective fading

Frequency selective fading occurs when the multipath fading is experienced at different frequencies across the channel at different levels. This causes both the phases and amplitudes of the signals to vary across the channel [2]. Sometimes relatively deep nulls may be experienced, and this can give rise to some reception problems. Simply maintaining the overall amplitude of the received signal will not overcome the effects of frequency selective fading, and some form of equalization may be needed. Some fading models are defined below [1]:

1. Rayleigh fading: Assumes isotropic scattering conditions, no line-of-sight [most common model], I- and Q-components of complex fading gain are complex, zero-mean Gaussian processes thus the fading envelope follows a Rayleigh distribution.

2. Ricean (Rice) fading: Assumes line-of-sight component is also present. I- and Q-components of complex fading gain are still complex Gaussian, but have non zero-mean thus the fading envelope follows a Rice distribution.

3. Nakagami-m fading: More general statistical model which encompasses Rayleigh fading as a special case, and can also approximate Ricean fading very well.

2.4.2 Relays

In wireless networks, usually there exists multiple nodes between the source and sink and the transmission is usually routed through these nodes. These intermediate nodes are termed as relays. There are many advantages of relays such as:

1. Transmission routing.

2. Relays can increase the transmission radius without increasing the transmit power.

3. In some cases, relays could check and eliminate transmission error before the sink.

The concept of cooperative relaying is introduced and Al-Yami [2], compared the diversity techniques for regenerative and non-regenerative relays:

- Regenerative relays (commonly referred to as decode and forward) decode the received data, check for errors and then retransmit it after encoding.

- Non-regenerative relays (commonly referred to as amplify and forward) just amplify the incoming transmission and forward the data without encoding and error checking.

So regenerative relays require processing but on the other hand they can detect the intermediate errors and request retransmissions at the intermediate level. On the other hand a non-regenerative node does not require sensitivity but it transmits the same data without error detection/correction. There can be more than 1 relay between transmitter and receiver. Each relay adds to the delay in transmission since each relay has to receive and

retransmit the same data. On the other hand relaying helps to increase the transmission range by enhancing the transmission power [9].

2.4.3 Error Control Schemes over Wireless Channels

It was discussed earlier that noise occurs in the environment which affects the communication by introducing errors in the packet. At the receiver, error detection is an important part for the integrity of the system. Since at the receiver there is no prior information of the received frame so error detection is very tricky. For error detection, many algorithms are used that send a pre-defined code with the frame that enables the receiver to quickly detect the errors. Following are the types of errors that occur in communication:

- Single Bit Error: 1 bit in error in a packet
- Multiple bit Error: Two or more random that are distributed over the bits in packet are in error
- Burst Errors: consecutive bits in packet are in error

Some of the codes that can be used for error detection in communication systems include:

2.4.3.1 Repetition codes

A repetition code is a coding scheme that repeats the bits across a channel to achieve error-free communication. Given a stream of data to be transmitted, the data are divided into blocks of bits. Each block is transmitted some predetermined number of times. A repetition code is very inefficient, and can be susceptible to problems if the error occurs

in exactly the same place for each. The advantage of repetition codes is that they are extremely simple.

2.4.3.2 Parity bits

A parity bit is a bit that is added to a group of source bits to ensure that the number of set bits (i.e., bits with value 1) in the outcome is even or odd. It is a very simple scheme that can be used to detect single or any other odd number (i.e., three, five, etc.) of errors in the output. An even number of flipped bits will make the parity bit appear correct even though the data is erroneous. Extensions and variations on the parity bit mechanism are horizontal redundancy checks, vertical redundancy checks, and "double," "dual," or "diagonal" parity (used in RAID-DP).

2.4.3.3 Checksums

A checksum of a message is a modular arithmetic sum of message code words of a fixed word length. The sum may be negated by means of a ones'-complement operation prior to transmission to detect errors resulting in all-zero messages. Checksum schemes include parity bits, check digits, and longitudinal redundancy checks.

2.4.3.4 Cyclic redundancy checks (CRCs)

A cyclic redundancy check (CRC) is a non-secure hash function designed to detect accidental changes to digital data in computer networks; as a result, it is not suitable for detecting maliciously introduced errors. It is characterized by specification of what is called a generator polynomial, which is used as the divisor in a polynomial long division

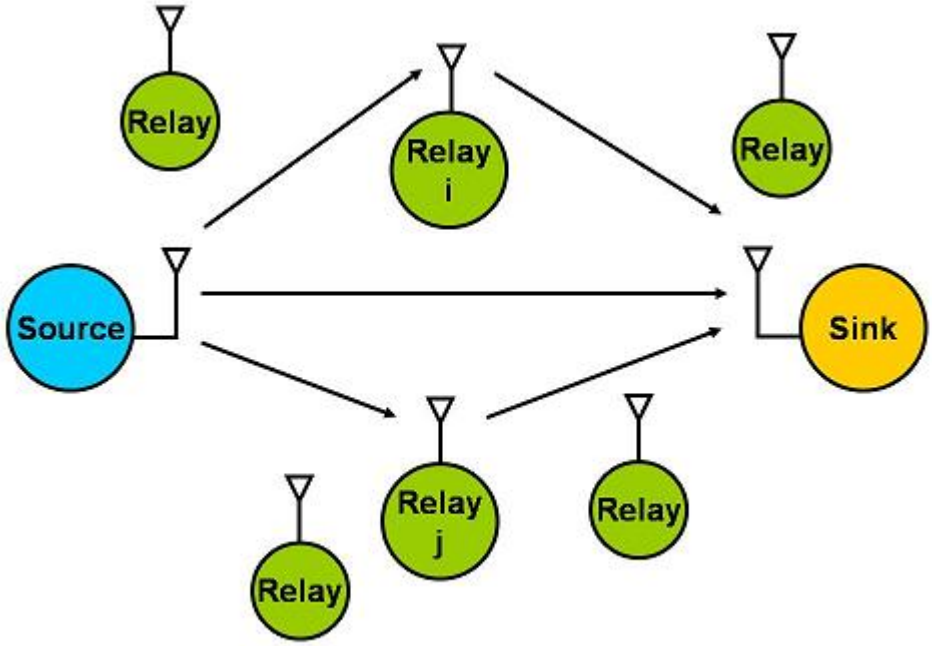


Figure 2.3: Relays between Source and Receiver Nodes

over a finite field, taking the input data as the dividend, such that the remainder becomes the CRC result. A cyclic code has favorable properties that make it well suited for detecting burst errors. CRCs are particularly easy to implement in hardware, and are therefore commonly used in digital networks and storage devices such as hard disk drives. Even parity is a special case of a cyclic redundancy check, where the single-bit CRC is generated by the divisor x + 1.

2.5 Diversity Techniques

At the receiver more than one copy of data maybe received. This is due to multipath fading environment and relays. A simple illustration can be seen in Fig. 2.3

The simple way is to select one copy and discard other copies. This can be done with

copies that are received at different times as with relays. But this mode is inefficient since many of the resources are wasted and the selected copy may have errors which may result in retransmission of the data. To avoid retransmission and increase Bit Error Rate (BER) diversity techniques are used that combine the incoming copies and generate best results. Following are the techniques that can be used.

2.5.1 Methods of Realizing Diversity Gain

Diversity techniques are used to mitigate degradation in the error performance due to unstable wireless fading channels, for example, subject to the multipath fading. Diversity in data transmission is based on the following idea: The probability that multiple statistically independent fading channels simultaneously experience deep fading is very low. There are various ways of realizing diversity gain [3], including the following ones;

2.5.1.1 Space Diversity

In this technique, sufficiently separated (more than 10 times the operating wavelength) multiple antennas are used to implement independent wireless channels.

2.5.1.2 Polarization Diversity

In polarization diversity, independent channels are implemented using the fact that vertically and horizontally polarized paths are independent.

2.5.1.3 Time Diversity

In time diversity, same information is repeatedly transmitted at sufficiently separated (more than coherence time) time instances.

2.5.1.4 Frequency Diversity

In frequency diversity, same information is repeatedly transmitted at sufficiently separated (more than coherence bandwidth) frequency bands.

2.5.1.5 Angle Diversity

In angle diversity, multiple receive antennas with different directivity are used to receive the same information-bearing signal at different angles.

2.6 Receiver Combining Schemes

In this section we present a discussion on the generative and non-regenerative cases of Maximum Ratio, Selective and Equal-Gain combining schemes. The specific statistical distribution(s) of h_{ij} would depend on the environment in which the network is deployed. In this case we consider the network in Figure 2.4. Detailed relations for each combining scheme for the regenerative and non-regenerative scenarios are given in the next section.

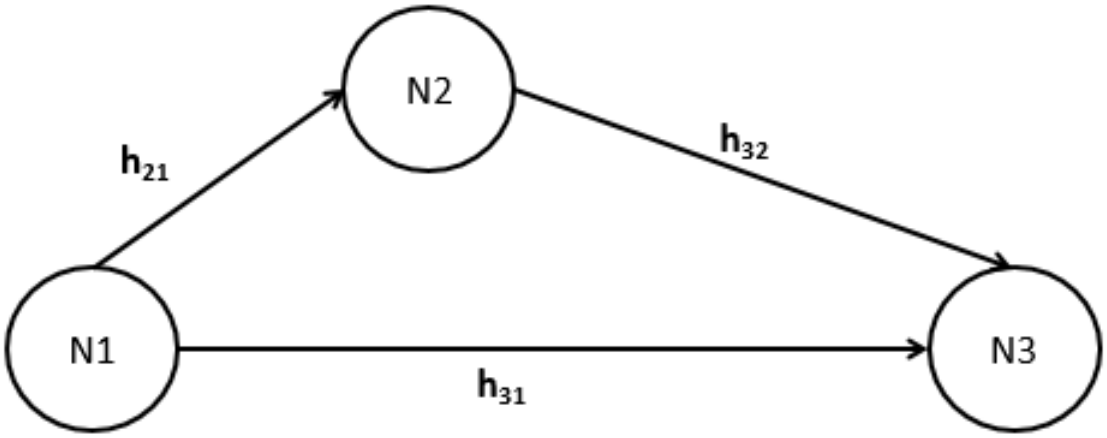


Figure 2.4: Diversity Combining Scenario

In this network a simple transmission scenario in which node 1 is acting as source and node 3 is acting as sink. Node 2 is the intermediate relay between the source and sink. Combining occurs at node 3 where there are 2 copies received. First copy is received directly from node 1 while the second copy is received through node 2. Node 2 is acting as regenerative or non-regenerative relay. The combining schemes used are maximum ratio combining (MRC), selection combining(SC) and equal gain combining(EGC).

2.6.1 Selection Combining - SC

In SC at the destination node, one of the two received copies is selected for detection while the selection criteria are the received SNR.

2.6.1.1 Non-regenerative system

Node 3 has two copies of the data, i.e., y_{31} and y_{32}. SNR is calculated for both the copies of signals as,

$$SNR_{31} = \frac{|h_{31}|^2}{N_0}, SNR_{32} = \frac{|h_{32}|^2 |h_{21}|^2}{|h_{32}|^2 N_0 + N_0}) \tag{2.1}$$

The selection criteria is given as

$$SNR = \max(\mathrm{SNR}_{31}, \mathrm{SNR}_{32}). \tag{2.2}$$

Based on criteria, one of the two copies is selected and the signal is detected.

2.6.1.2 Regenerative system

This technique is the same as for non-regenerative systems, however, the SNR values are changed since node 2 is now resorting to decode-and-forward. At node 3, SNR is calculated for both the copies, i.e., y_{31} and y_{32}. Where the SNR's are given by

$$SNR_{31} = \frac{|h_{31}|^2}{N_0}, SNR_{32} = \frac{|h_{32}|^2}{N_0}, \tag{2.3}$$

and the selection criteria is

$$SNR = max(SNR_{31}, SNR_{32}) \tag{2.4}$$

Based on this criteria, one of the two copies is selected and the signal is detected.

2.6.2 Maximum Ratio Combining - MRC

2.6.2.1 Non-regenerative system

In MRC at the destination node, both copies are combined using the matched filter, which is optimal in the sense of maximizing the signal to noise ratio (SNR). y_{21} is the received data at node 2, z_{21} is the additive Gaussian noise and x_1 is the transmitted data. Node 2 processes the received signal in a non-regenerative manner as given as,

$$y_{21,NG} = \frac{h_{21}^*}{|h_{21}|^2} y_{21} = |h_{21}| x_1 + \frac{h_{21}^*}{|h_{21}|^2} z_{21}, \tag{2.5}$$

Where $y_{21,NG}$ is amplified and transmitted again by node 2. This strategy termed as amplify-and-forward and marred by the amplification of noise. Node 3 receives two copies of data. The direct copy from sensor node 1 is given as

$$y_{31} = h_{31} x_1 + z_{31}, \tag{2.6}$$

while the indirect copy from node 2 is given as

$$y_{32} = h_{32} y_{21,NG} + z_{32}, \tag{2.7}$$

Where y_{31} is the received data from node 1 and y_{32} is the data received from node 2.

Node 3 combines these two copies of data as

$$y_{3,NG} = \frac{h_{31}^*}{|h_{31}|^2 + |h_{32}|^2} y_{31} + \frac{h_{32}^*}{|h_{31}|^2 + |h_{32}|^2} y_{32}. \tag{2.8}$$

The received SNR at the destination node is given in [11, 12] as

$$\text{SNR} = \frac{|h_{31}|^2 + |h_{32}|^2 |h_{21}|^2}{|h_{32}|^2 N_0 + N_0}. \tag{2.9}$$

2.6.2.2 Regenerative system

This scheme is expected to have better performance than the non-regenerative systems since noise effect is canceled by the decoding at the intermediate node [11]. Node 2 processes the received signal y_{21}, given by,

$$y_{21,RG} = \frac{h_{21}^*}{|h_{21}|^2} y_{21} = |h_{21}| x_1 + \frac{h_{21}^*}{|h_{21}|^2} z_{21}. \tag{2.10}$$

It then decodes the signal x_1. The recovered signal is then retransmitted, thereby canceling the effect of noise at node 2. The received signal at the destination node is combined as

$$y_{3,RG} = \frac{h_{31}^*}{|h_{31}|^2 + |h_{32}|^2} y_{31} + \frac{h_{32}^*}{|h_{31}|^2 + |h_{32}|^2} y_{32}, \tag{2.11}$$

where the received SNR is given as

$$\text{SNR} = \frac{|h_{31}|^2 + |h_{32}|^2}{N_0 + N_0}. \tag{2.12}$$

Note that combining here must occur offline because of the delay in one path compared to the other.

2.6.3 Equal Gain Combining - EGC

In EGC, each copy is multiplied by an equal gain and then all copies are added coherently. Though the scheme is suboptimal, but it avoids the non linear region of power amplifiers and is considered to be hardware friendly.

2.6.3.1 Non-regenerative system

At node 3, the two received signals are y_{31} and y_{32}. Node 3 combines these two copies of data as

$$y_{3,NG} = \frac{h_{31}^*}{|h_{31}|} y_{31} + \frac{h_{32}^*}{|h_{32}||h_{21}|} y_{32}, \tag{2.13}$$

and $y_{3,NG}$ is then used to detect the signal. The received SNR [13, 12] is given as

$$\text{SNR} = \frac{|h_{31}|^2 + |h_{32}|^2}{N_0 \left(\frac{1}{|h_{31}|^2} + \frac{1}{|h_{32}|^2 |h_{21}|^2} + \frac{1}{|h_{32}|^2 |h_{21}|^2} \right)}. \tag{2.14}$$

2.6.3.2 Regenerative system

The technique is the same as for EGC for non-regenerative systems. Node 3 combines the two copies of data as

$$y_{3,RG} = \frac{h_{31}^*}{|h_{31}|} y_{31} + \frac{h_{32}^*}{|h_{32}|} y_{32}. \tag{2.15}$$

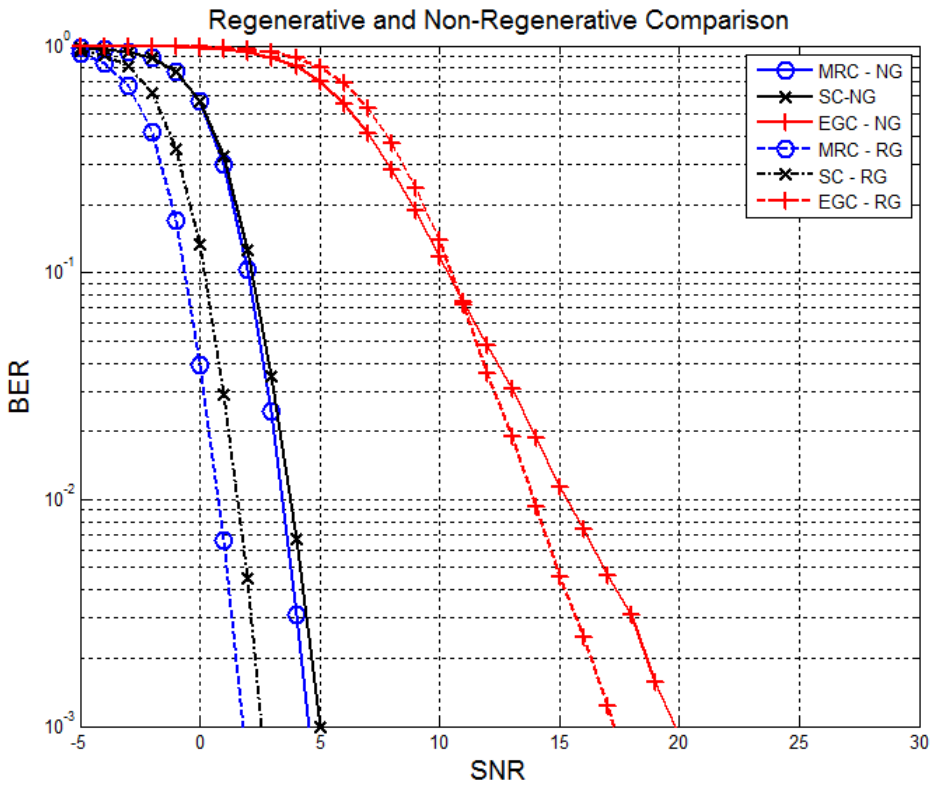


Figure 2.5: BER of diversity techniques with regenerative and non-regenerative systems

The received SNR [9, 13] is given by

$$\text{SNR} = \frac{4}{N_0\left(\frac{1}{|h_{31}|^2} + \frac{1}{|h_{32}|^2}\right)}. \tag{2.16}$$

The results with regenerative and non-regenerative relay are shown in Figure 2.5.

We can observe from the BER plot that, the MRC-RG outperforms all the combining schemes. This is followed by the SC-RG. The BER curves for MRC-NG and SC-NG then follow in performance. These appear to be similar with about less than 1dB difference. From the results, we also observe that the MRC-RG is about 3dB better than the MRC-NG. Similarly, SC-RG outperforms the SC-NG by about 3dB. The equal gain techniques registered the worst results as compared to all other schemes. The EGC-RG is observed

to be about 2dB better than that of EGC-NG. Hence as expected, the regenerative techniques always outperforms the non-generative techniques.

A comprehensive work is done on fading channels while using diversity techniques. In [3] authors compared the generalized fading channel on select combining scheme. Work is also done on comparison of diversity techniques on Rician fading channel [4]. In [5] and [6], the authors compared the diversity scheme effect on Rayliegh and Nakagami fading channels.

CHAPTER 3

COMBINING SCHEMES FOR RELAY-BASED DIVERSITY IN FADING CHANNELS

This chapter delves into the performance of cooperative wireless sensor networks in fading prone environments. Here, we adopt a certain network configuration and model each network link as a specific fading distribution. We then conduct a series of simulations based on the modeled network to evaluate the performances of MRC, SC and EGC and compare their performances with our developed error correction technique. The chapter resorts to two metrics, i.e., bit error rate (BER) and frame error rate (FER) for the performance evaluation for all schemes in our simulations.

3.1 Combining Schemes over Relay-Based Fading Channels

In the literature review we have seen the comparison of diversity techniques using regenerative and non-regenerative relays. The non-regenerative relays usually amplify the noise and thus give higher bit and packet error rates. A scenario is created that is shown in Figure 3.1. In Figure 3.1, there are 4 nodes in which node 1 acts as source and node 4 acts as sink. Node 2 and node 3 are acting as intermediate relays which could be generative and non-regenerative. h is the transfer function between nodes and z is the noise between the intermediate nodes.

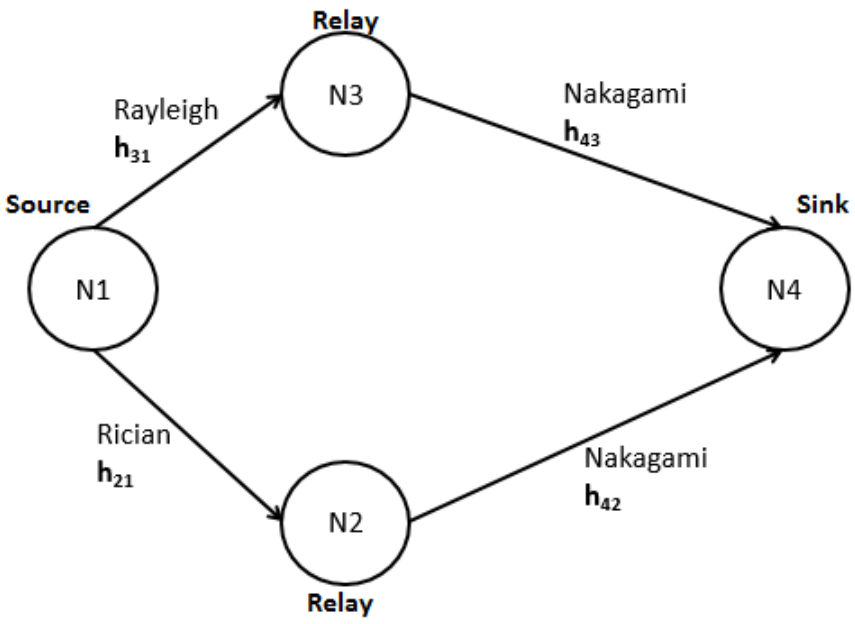


Figure 3.1: Simulation Scenario

This scenario assumes different channel fading models in each communication link. QPSK modulation is used for that scenario. Since in real world scenarios there could

be different kinds of fading between different nodes, the fading coefficient between the source and relays are modeled as Rayleigh and Rician distributions while that between the relays and receiver are modeled as Nakagami distributions.

Now,

$$y_{21} = h_{21}x + z_{21} \tag{3.1}$$

$$y_{31} = h_{31}x + z_{31} \tag{3.2}$$

$$y_{42} = h_{42}y_{21} + z_{42} \tag{3.3}$$

$$y_{43} = h_{43}y_{31} + z_{43} \tag{3.4}$$

where,

y_{ij} = Signal received at node i and node j

z_{ij} = Additive noise between node i and node j

h_{ij} = Fading transfer function between node i and node j

When node 2 and 3 are acting as regenerative relays the packet is received and decoded at the intermediate nodes. In case of successful reception the packet is again encrypted and sent to node 4. If the packet is erroneous at any of the nodes, then retransmission occurs. Diversity combining occurs at sink (node 4) we have simulated the following

diversity schemes for regenerative and non-regenerative nodes.

1. Maximum Ratio Combining (MRC)

2. Equal Gain Combining (EGC)

3. Selection Combining (SC)

For each combining scheme, a QPSK based communication system is designed based on Figure 3.1 and the corresponding combining equations are presented. Simulations are then carried out and Bit Error Rate (BER) and Frame Error Rate (FER) results are compared so as to evaluate performance. This is done for both regenerative and non-regenerative schemes.

3.2 Simulation Results for Combining Schemes

In this section we conduct simulations for each scheme based on the stated relations. The QPSK modulation scheme is used in all simulations. The results for BER and FER against SNR at receiver are generated for each combining scheme and compared.

3.2.1 Regenerative Relay Communication

Regenerative relays receive the incoming transmission, decode it, and check for errors. If errors exist in the incoming transmission, they will request retransmission; otherwise the packet is transmitted to next hop.

It can be seen that as the SNR goes higher BER and FER start to decrease. The FER represents the probability that a frame being transmitted is in error. This is nearly

inversly proportional to the SNR.

The BER vs SNR and FER vs SNR results are shown in Fig. 3.2 and 3.3 respectively. It can be seen that the MRC is showing best result since the gain is added with respect to the noise it contains. As a result noise is not amplified and gives best result at minimum SNR. Since since EGC adds equal noise to all the copies, as a result noise get amplified and gives poor results.

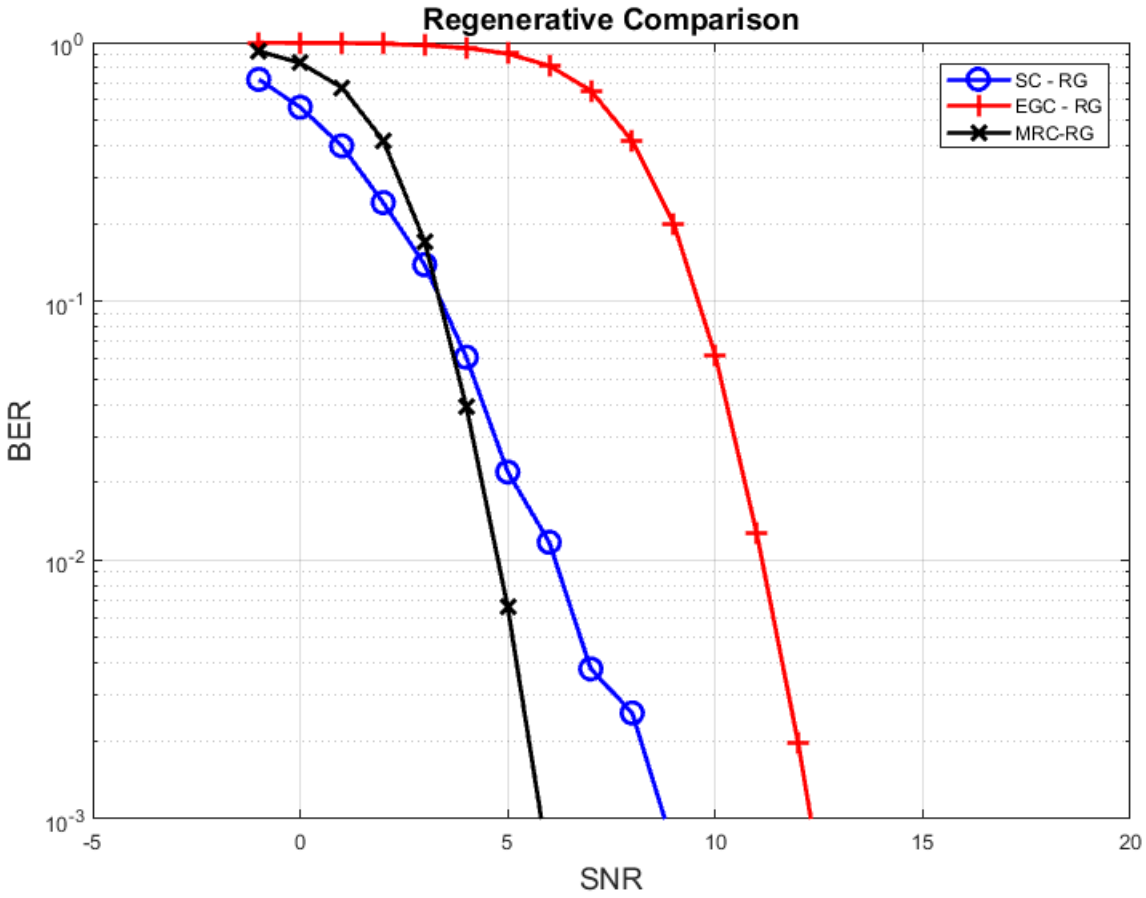


Figure 3.2: BER vs SNR comparison of Regenerative Relays

As it can be observed, for the regenerative relay based system, an SNR of 6dB, 7.9dB and 12.5dB are required to reach a Bit Error Rate (BER) of 10^{-3} for MRC, SC and EGC respectively. Likewise, for a Frame Error Rate (FER) of 10^{-2} an SNR of 9dB, 12.2dB

and 13.8dB for MRC, SC and EGC. Hence it can be inferred that, for the regenerative system, the MRC produces the best results followed by SC and then EGC.

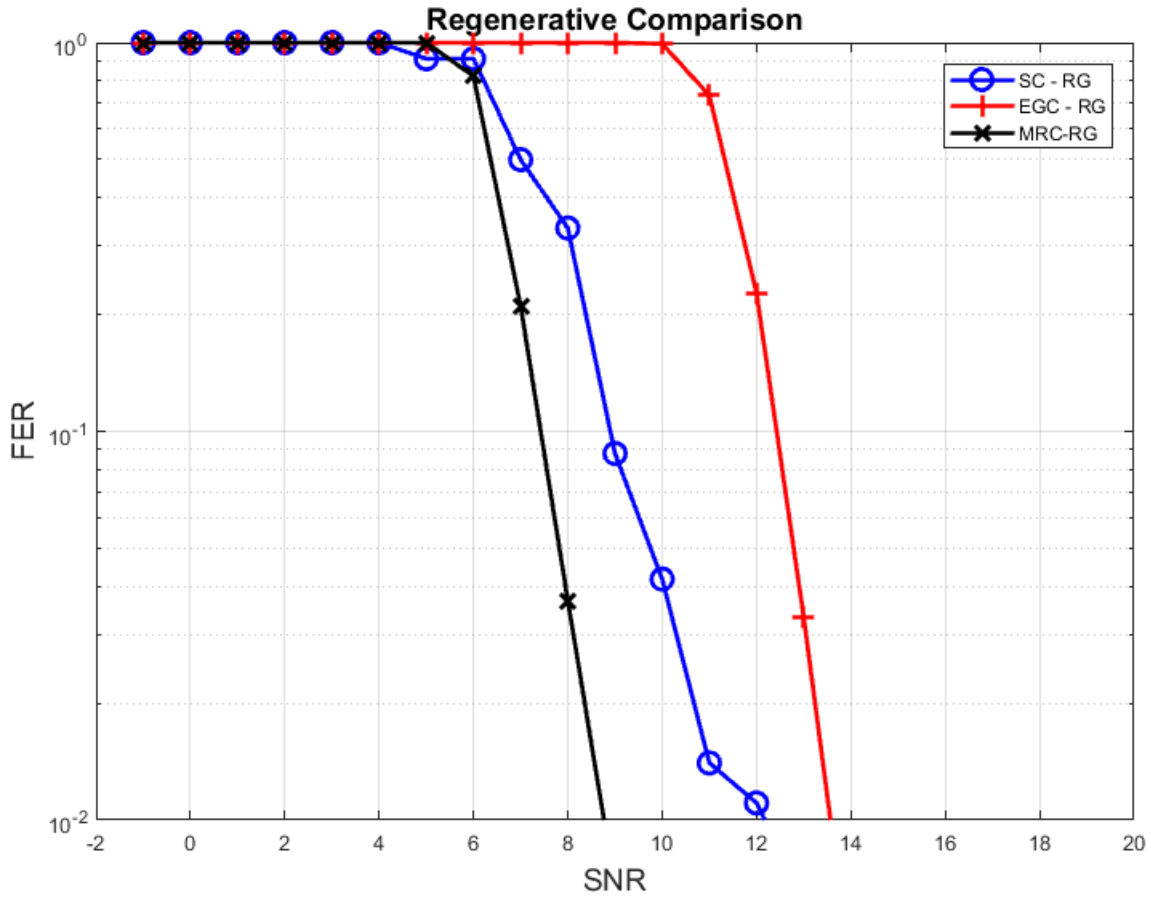


Figure 3.3: FER vs SNR diversity comparison of Regenerative Relay

3.2.2 Combining Schemes and Non-Regenerative Relay Communication

For non-regenerative relays the intermediate relay receives a packet, amplifies it, and then further sends it to the sink node. The output equation will remain the same but since the packet is not decoded so the additional noise is also amplified with the packet. Figures 3.4 and 3.5 shows the comparison of diversity schemes with non-regenerative relays.

As it can be observed, for the non-regenerative relay based system, an SNR of 10.8dB, 12.3dB and 14dB are required to reach a Bit Error Rate (BER) of 10^{-3} for MRC, EGC and SC respectively. Likewise, for a Frame Error Rate (FER) of 10^{-2} an SNR of 12.5dB, 15.8dB and SNR more than 15dB for MRC, SC and EGC respectively. Hence it can be inferred that, for the regenerative system, again the MRC produces the best results followed by SC and then EGC.

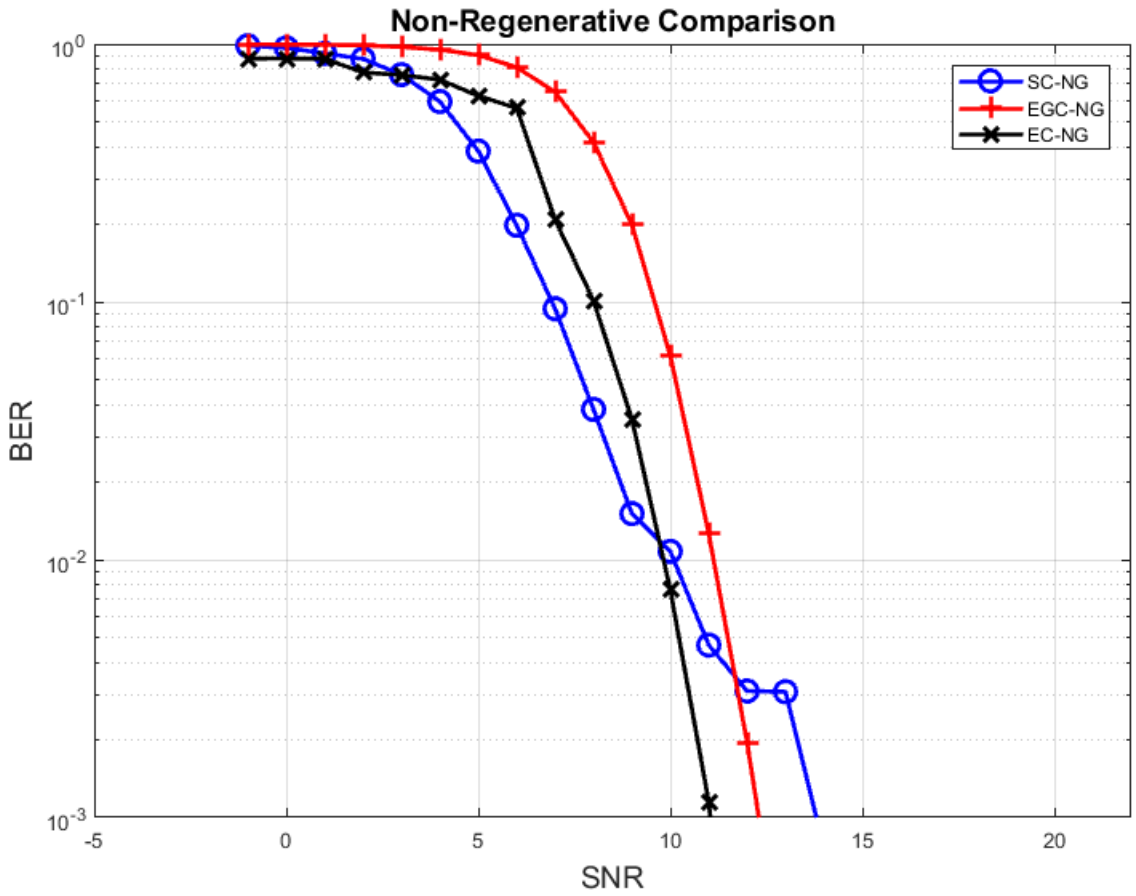


Figure 3.4: BER vs SNR comparison of Non-Regenerative diversity techniques

MRC again proved to be the best among the three schemes. Since selection combining takes into account the SNR best available so it is better than equal gain combining.

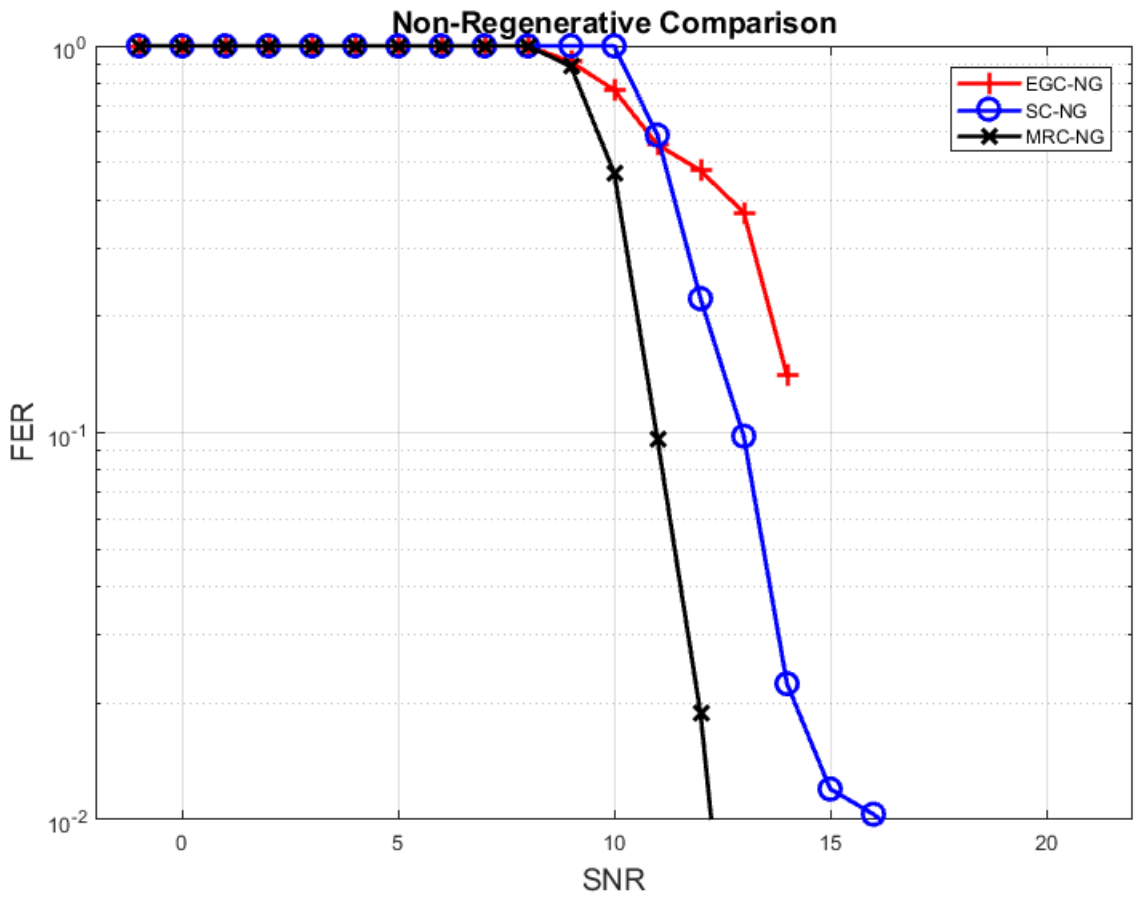


Figure 3.5: FER vs SNR comparison of Non-Regenerative diversity techniques

Figure 3.6 and Figure 3.7 compare the BER and FER curves of EGC, MRC and SC for regenerative and non-regenerative relays. The behavior of each kind of diversity scheme is similar. The difference is where the bit and frame error rate starts going towards zero.

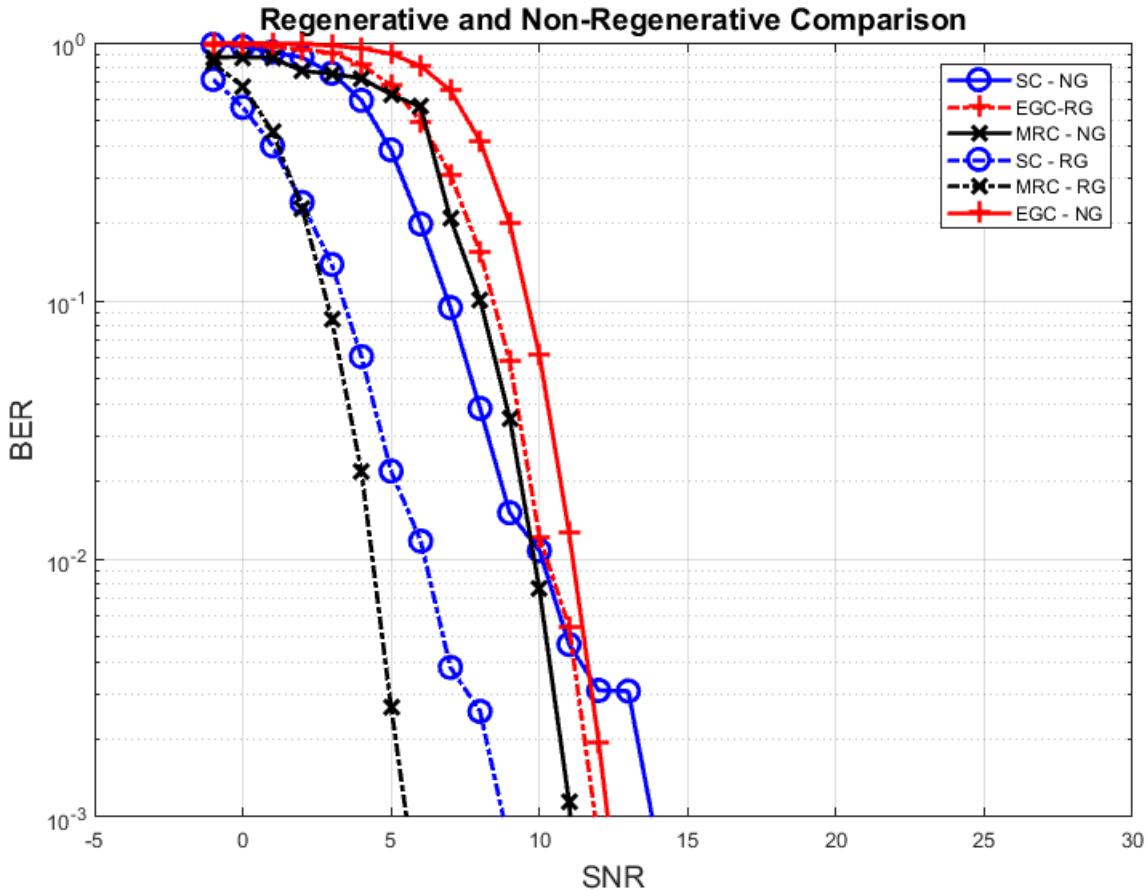


Figure 3.6: BER vs SNR Comparison of Regenerative and Non-Regenerative Schemes

In the regenerative relay system, since the intermediate noise and errors are catered for first at the relays, they give a better performance as compared to the non-regenerative relay system. The non-regenerative relay system on the other hand, amplifies the noise, which causes performance degradation.

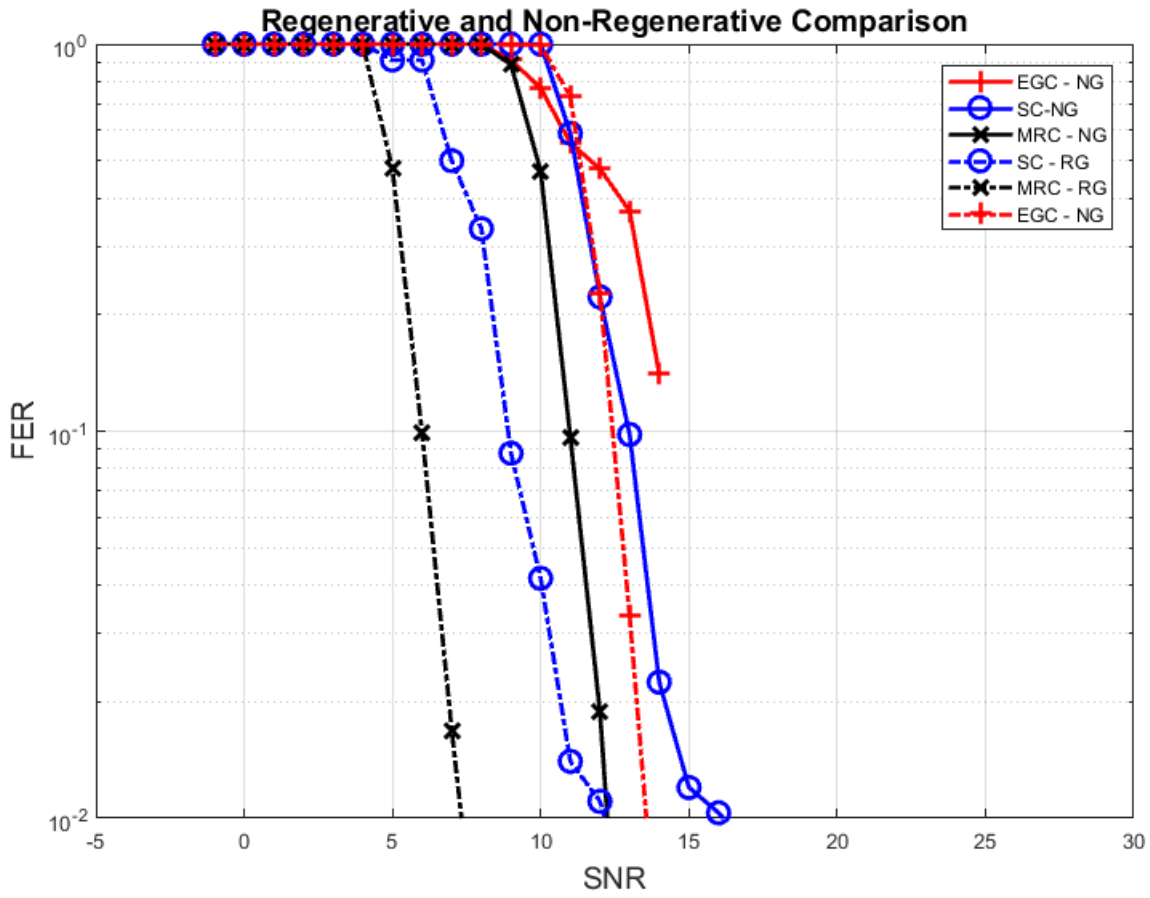


Figure 3.7: FER vs SNR Comparison of Regenerative and Non-Regenerative Schemes

3.3 Error Correction as a Technique for Diversity

Based on the CRC check and multiple path fading, an error correction technique is devised which will check and correct errors. The receiver will be designed as shown in Figure 3.9.

Assume that we have a communication system that to transmits frames of length, N bits. Assuming that frames in a WSN are transmitted over two paths. Given that the Signal-to-Noise Ratios (SNRs) in the two paths are SNR_1 and SNR_2 and the probability of bit error in a frame in the two paths is P_{b1} and P_{b2}, which are given by;

$$P_{b1} = \frac{1}{2} erfc(\sqrt{SNR_1}), \text{ and} \tag{3.5}$$

$$P_{b2} = \frac{1}{2} erfc(\sqrt{SNR_2}) \tag{3.6}$$

A frame is said to be in error if one or more bits are flipped in the frame or a frame is lost during transmission.Hence the probability that a frame of length, N is in error in the two paths, P_{F1} and P_{F2},

$$P_{F1} = 1 - (1 - P_{b1})^N \tag{3.7}$$

$$P_{F2} = 1 - (1 - P_{b2})^N \tag{3.8}$$

Assuming the two paths over which the frames are transmitted are independent, a frame will be received with errors that would require retransmission only if the two received copies of the frame as they were transmitted over the two paths both had errors, i.e.,

$$P[Both\ copies\ of\ a\ frame\ are\ in\ error] = P[Frame\ 1\ is\ in\ error] \times P[Frame\ 2\ is\ in\ error]$$

$$P[Both\ copies\ of\ a\ frame\ are\ in\ error] = [1 - (1 - P_{b1})^N] \times [1 - (1 - P_{b2})^N] \tag{3.9}$$

Assuming in any transmission, the probability that there are i errors in frame 1 and the probability that there are j errors in frame 2 are given respectively as;

$$P_{F1}^i = \binom{N}{i} P_{b1}^i (1 - P_{b1})^{N-i} \tag{3.10}$$

$$P_{F2}^{j} = \binom{N}{j} P_{b2}^{j} (1 - P_{b2})^{N-j} \tag{3.11}$$

Hence, the probability of having i errors in Frame 1 and j errors in Frame 2 in a particular transmission is given by;

$$P^{i,j} = P_{F1}^{i} \times P_{F2}^{j}$$

Say we can design a coding system that can correct up to n_E errors in the two frames in a particular transmission, for the event generating, $P^{i,j}$, the probability of having any number of errors up to n_E in the two received frames can be given by;

$$P = \sum_{i=2}^{n_E} \sum_{j=2}^{n_E} P^{i,j} \tag{3.12}$$

In Figure 3.8 we show theoretical performances of a QPSK scheme given by Equation 3.5 and 3.6 representing the BER and FER respectively for $N = 100$ and $n_E = 20$.

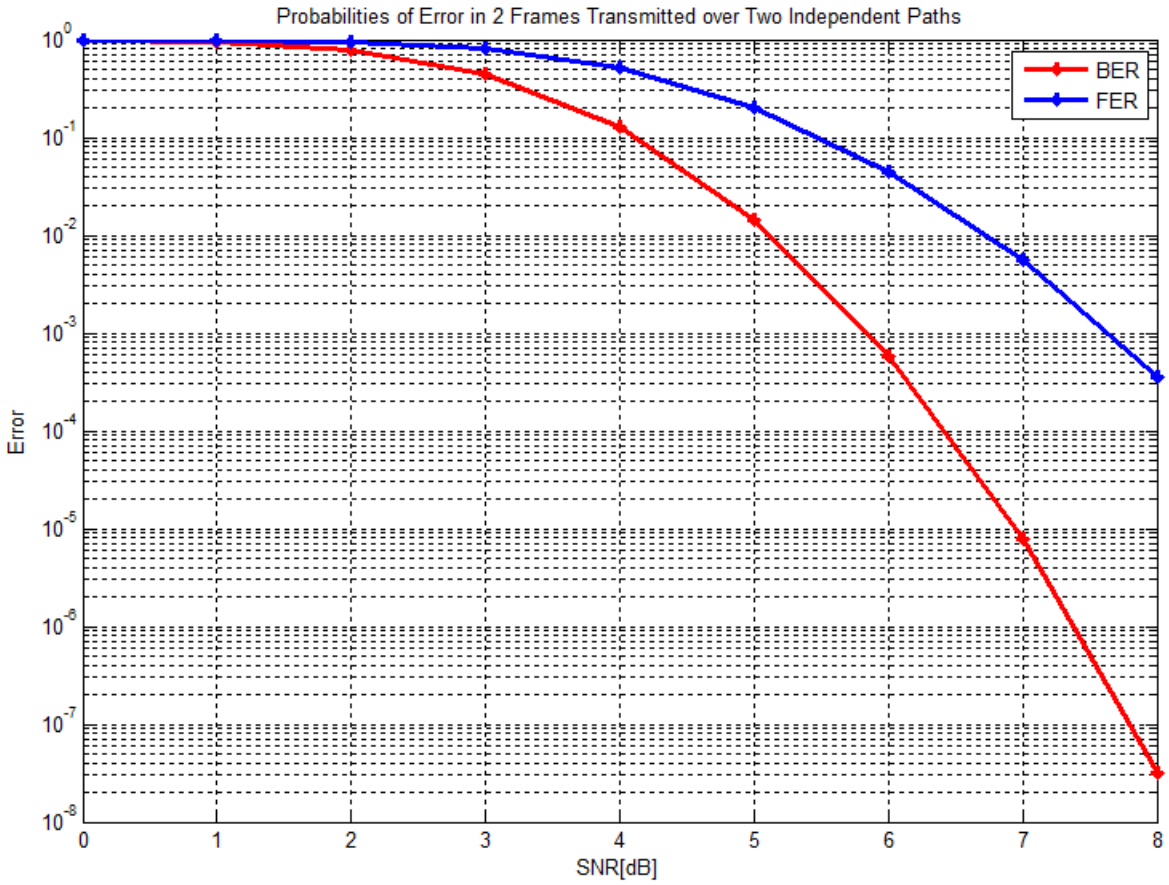


Figure 3.8: Theoretical BER and FER for $N = 100$ and $n_E = 20$

This theoretical results presents a fair idea as to how best a correction scheme can perform in a dual-path communication for cooperative WSNs. The performance of our correction scheme could be matched against the theoretical results to know its accuracy with increasing values of SNR.

Say, two packets are received at a destination node, instead of combining, the receiver will decode these packets separately and will apply the CRC check. In case of success with any of them, the received packet that satisfies the CRC check is assumed to be correct and hence a successful transmission. If the CRC check fails with both of the received packets, a bit-wise XOR operation is applied that will identify any bit differences in

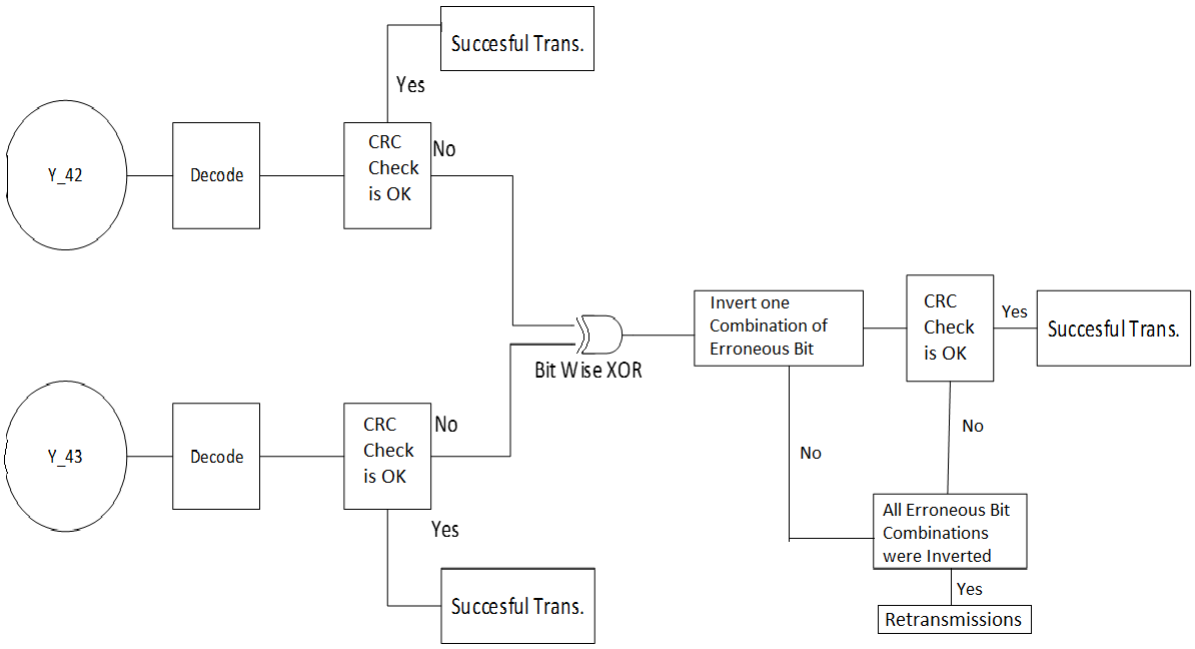


Figure 3.9: Error Detection and correction receiver

the two receive packets. The XOR operation gives a logical '1'at its output in case any differences are detected. Whenever there a is '1'at the output of the XOR, it means there is an error in one of the received packets or errors in both packets occurring at different bit positions. We can simply invert the bits that differ in the two packets and then re-conduct a CRC check. If after the CRC check, no error is detected, the packet is assumed to have been corrected and hence a reduction in the number of retransmissions is achieved. In case there are still errors in the corrected frame, different combinations of bits are inverted and the process is repeated until either a correct packet is found or a maximum number of iterations is reached. Applying this algorithm could significantly reduce retransmissions.

We can use both type of relays i.e. regenerative and non-regenerative relays with this technique at the intermediate node. This technique could also be used at the intermediate

node if multiple copies are received at the relay.

To elaborate further on this technique, consider a communication scenario where a source (N1) transmits to two intermediate or relay nodes (N2 and N3). The two relay nodes (N2 and N3) then transmit to destination node (N4). This scenario is illustrated in Figure 3.1. If a simple CRC check is used for the detection of errors, and retransmissions are requested if errors occur, assume that N1 transmitted one packet to N2 and N3, and both of the received packets had one or two bit errors. It is valid to assume that generally errors will occur in the two received packets at different locations. As described earlier, in the case of regenerative transmission, nodes N2 and N3 will not forward these erroneous packet but will request re-transmission whereas in the non-regenerative transmission case, nodes N2 and N3 do not request retransmission and send the erroneous packets to the destination node, N4. Regardless of the mode, assume the erroneous packets are received at node N4. N4 then conducts a search by comparing the received erroneous packets. More errors are expected to occur in these packets since their transmission occur over two different links. Node N4 then does a reversal of bits that differ in the two packets in one of the packets and CRC check is performed again. If this packet passes the CRC test, there is a high probability that the packet has been corrected and hence there's no need for retransmission(s).

This scenario is as summarized below. Erroneous bits are indicated by a 'cap'.

1. N1 transmits '101101001', followed by CRC check '101'

2. N2 receives '1011$\hat{1}$001', followed by CRC check '1$\hat{1}$1'. If N2 checks, it will see that the packet is erroneous. Similarly, N3 Receives '10110101$\hat{1}$1', followed by CRC check

'101'. Likewise, N3 sees an erroneous packet after the check.

3. N4 receives from N2 '1$\hat{1}$111$\hat{1}$1001', followed by CRC check '1$\hat{1}$1'(if N4 checks, it will see that the packet is erroneous). N4 receives from N3 '10110101$\hat{1}$1', followed by CRC check '101'(if N4 checks, it will see this packet to be erroneous).

4. By comparing the packets received from nodes N2 and N3, N4 can detect places of errors (unless errors occur at the same place in both received packets which is highly unlikely for reasonable error rates). In effect, N4 will detect the locations of errors to be the ones marked with X.

   1X11X10X1 followed by CRC check 1X1

5. The receiver N4 will have to assume that some of the errors belong to the first packet and the remaining belong to the second, and hence both are in error.

6. Now, N4 will have to do a reversal of the bits marked with X (i.e., a maximum of $\sum_{i=1}^{k-1} \binom{k-1}{i}$ trials in this case, where k is the number different bits between the two frames). After each bit reversal, the CRC is used to check to see if the new packet is correct. If so, successes, otherwise try the next case and so on. Obviously, if the number of bit errors is low, i.e., 1, 2, 3 , 4 and up to say 6 or 7, this process can be carried out without much difficulty, and will alleviate or minimize retransmissions and hence saving sensor node power which is prime in the operation of wireless sensor networks. In addition it will save valuable power that would be wasted in requesting retransmissions and relaying these transmission

requests back to sensor nodes. Despite this feature, this technique will perform not in communication environments where the number of bit errors in packets are enormous or in situations where bit errors occur at the same location in both received packets. In these situations, retransmissions can be requested.

CRC is chosen here for error detection so as to avoid the transmission of additional information at the expense of slightly increasing the complexity of the system. Other robust error control codes like, Reed-Solomon coding or turbo coding will further increase the complexity of the communication system and the packet overhead hence make them inefficient in terms of minimization of node power consumption.

Further, since this technique drastically reduces the number of retransmissions in every communication cycle as compared to the other combining schemes, it is expected to outperform the other techniques.

In Figures 3.10 and 3.11, we compare the performance in terms of BER and FER respectively, of the error correction technique for the regenerative and non-regenerative scenarios for a frame size of 100 bits where we try to correct up to 10% of the frame bits for each simulation.

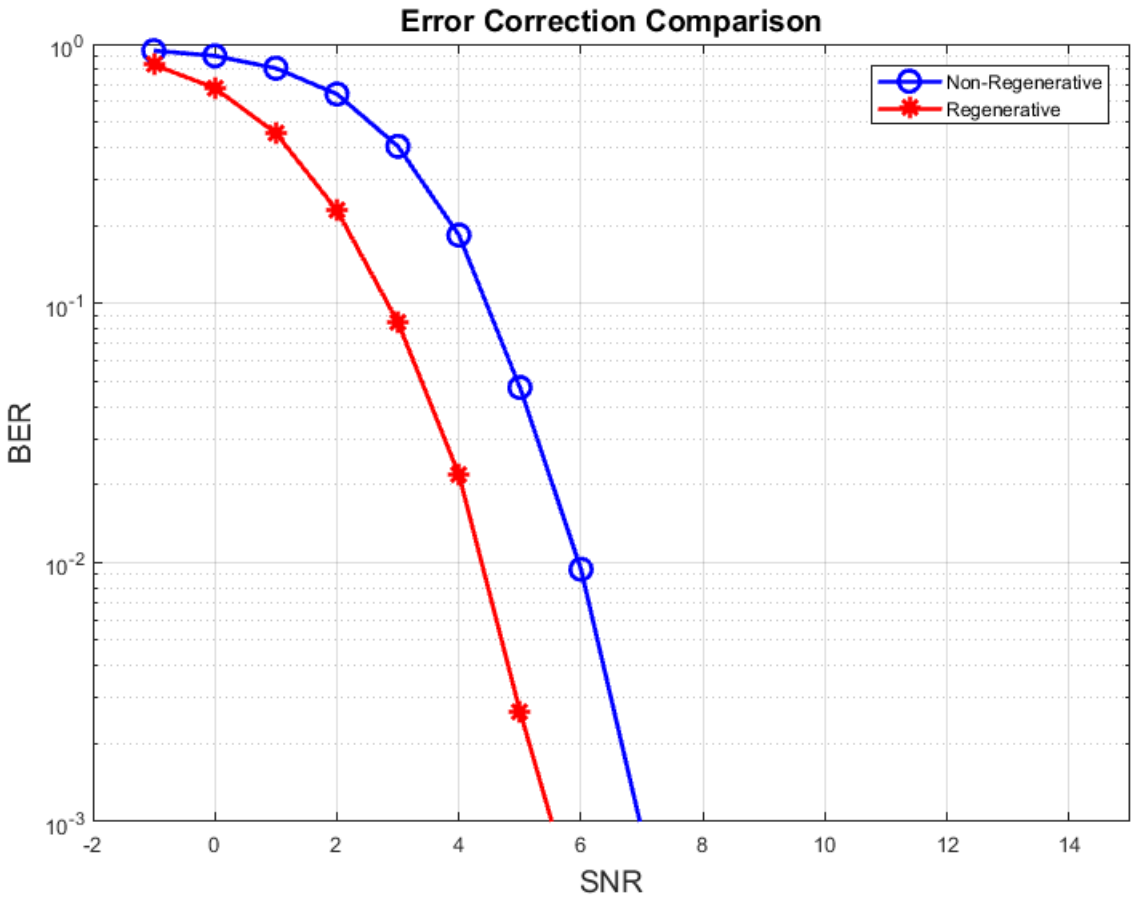


Figure 3.10: BER vs SNR curve for Error Correction Technique

As expected, the regenerative system outperformed the non-regenerative system in both FER and BER. This is because the packet from N1 is checked for errors at the intermediate relay nodes (N2 and N3) so the probability of error is less than that of non-regenerative relay.

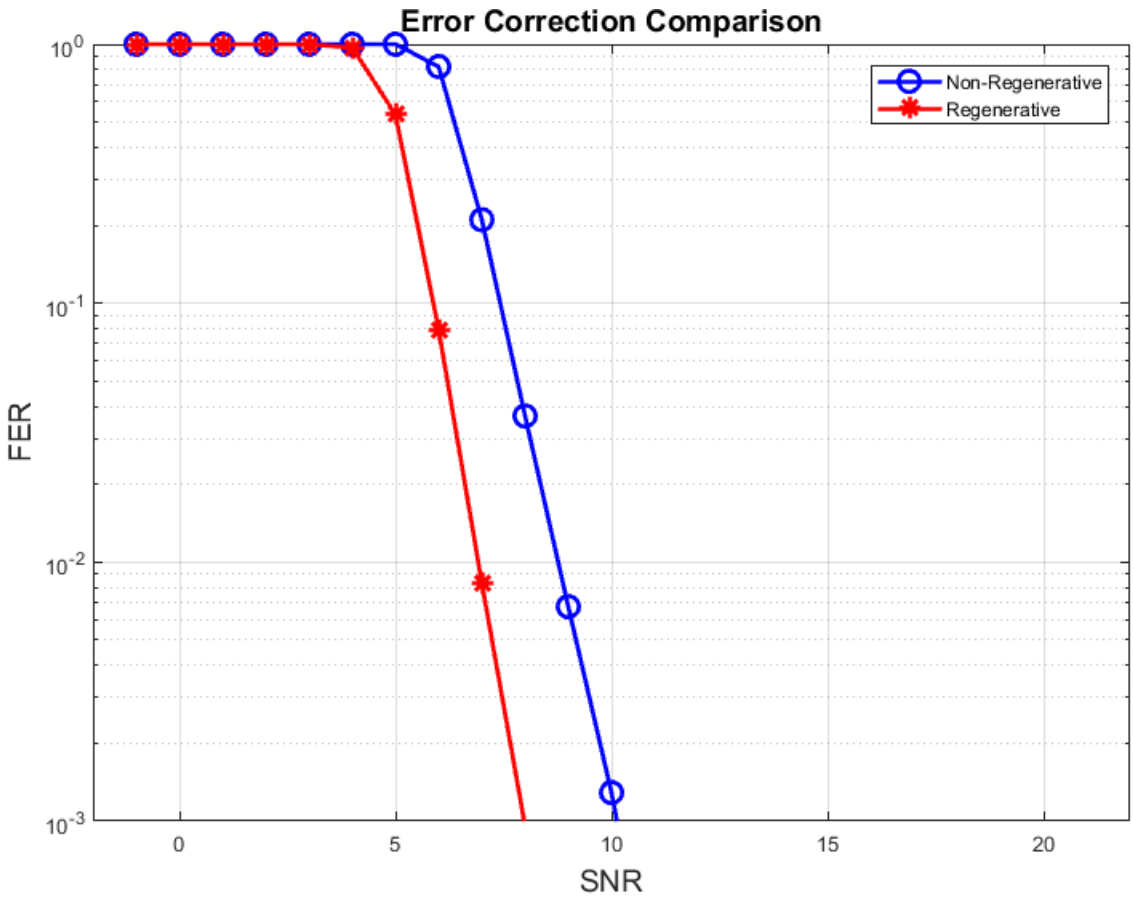


Figure 3.11: FER vs SNR curve for Error Correction Technique

We also compare the derived error correction technique with the diversity schemes simulated above. The diversity tends to remove error by employing the best SNR from the received packets. While the discussed error correction technique separately interprets each of the received packet and check for error after decoding the packet. If error exists, it will employ the error correction technique. Figure 3.12 and Figure 3.13 compares the error correction technique with the diversity schemes.

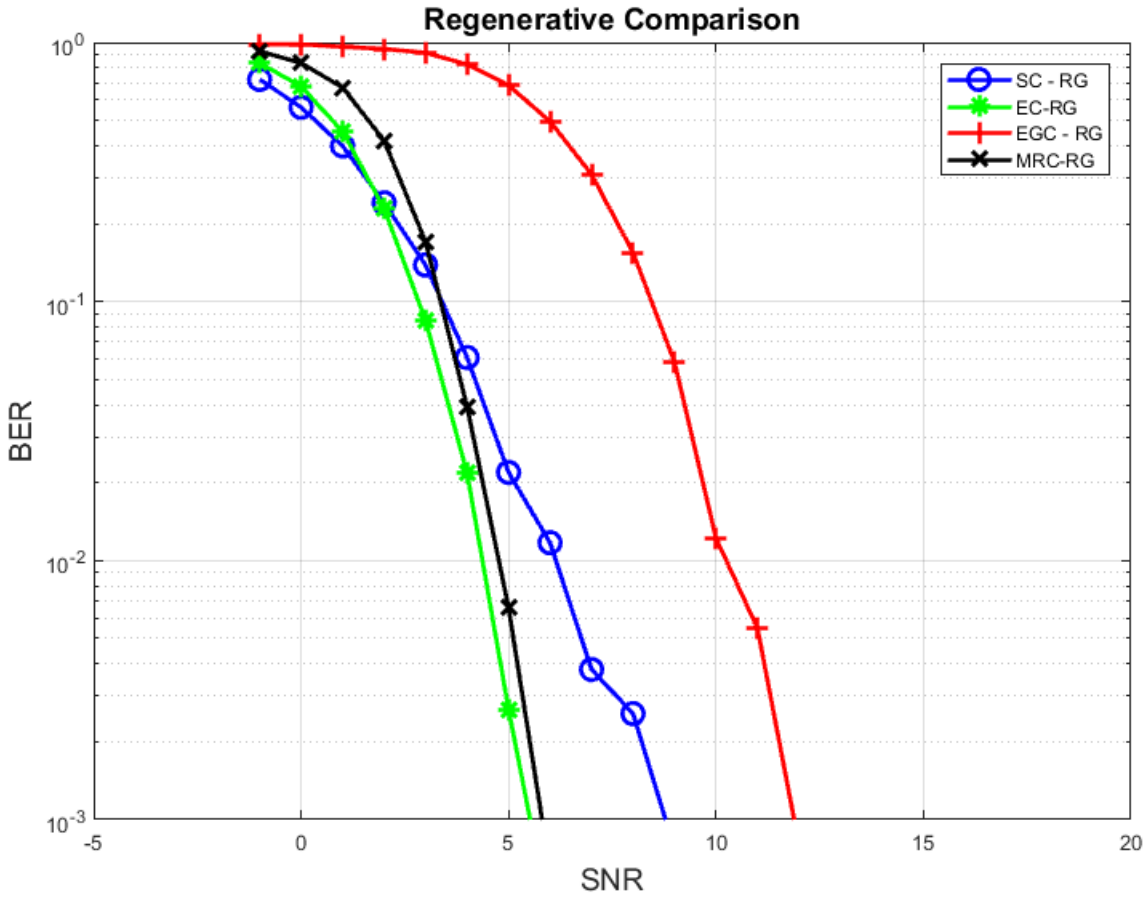


Figure 3.12: Error correction vs diversity for regenerative Relays

It can be observed, for the regenerative relay based system, an SNR of 5.7dB, 5.9dB, 8.5dB and 12dB are required to reach a Bit Error Rate (BER) of 10^{-3} for the Error Correction technique, MRC, SC and EGC respectively. Hence it can be inferred that, for the regenerative system, the error correction technique is better than all the SNR based combining techniques. This is largely due to the fact that the error correction technique minimizes the number of retransmissions in communication as compare to the MRC, EC and EGC schemes.

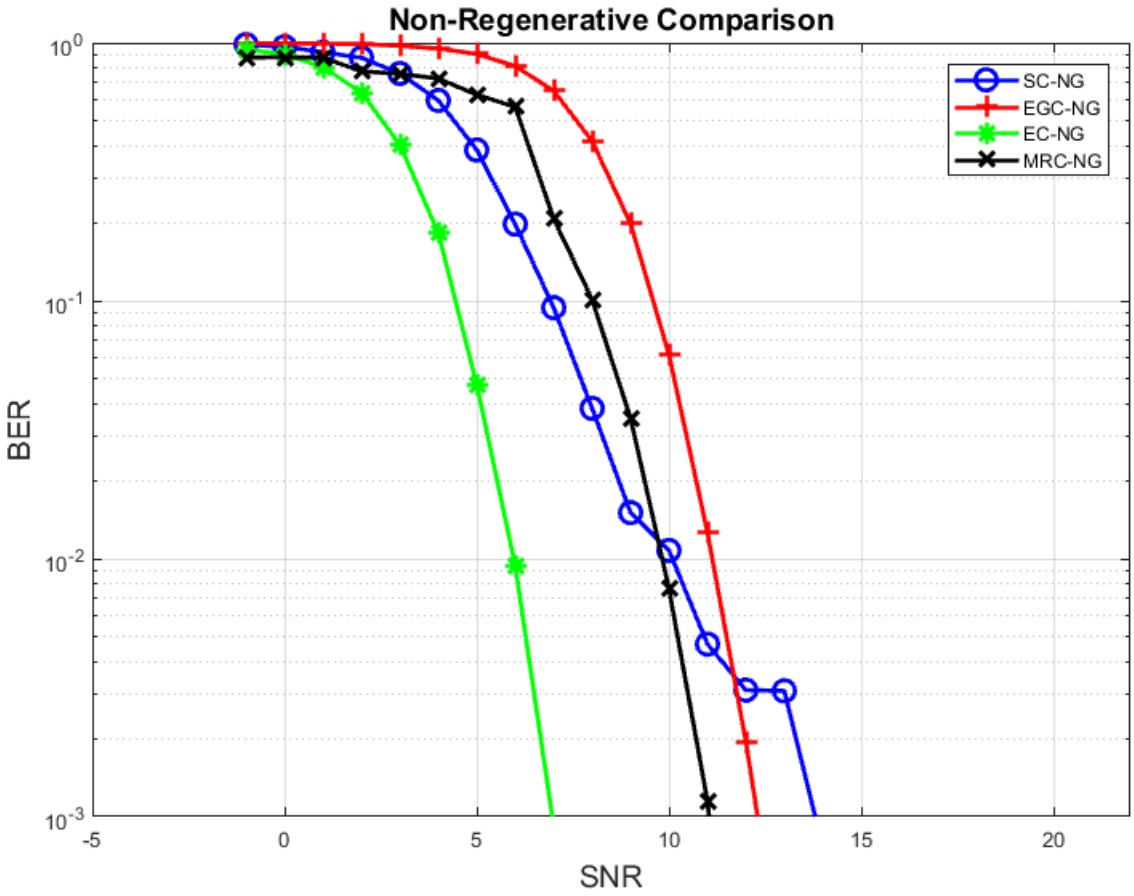


Figure 3.13: Error correction vs diversity for non-regenerative Relays

Similar to the regenerative results, it can be observed, for the non-regenerative relay based system, an SNR of 7dB, 11dB, 12dB and about 13.5dB is required to reach a Bit Error Rate (BER) of 10^{-3} for the Error Correction technique, MRC, EGC and SC respectively. Hence it can also be inferred that, for the non-regenerative system, the error correction technique outperforms the MRC, SC and EGC systems in terms of BER and FER. All regenerative techniques outperform their corresponding non-regenerative techniques in terms of BER and FER.

CHAPTER 4

EXPERIMENTAL WORK

In this section, we present a real time experimental evaluation of Zigbee, WirelessHART and ISA100-based systems. The appropriate topologies are generated for each test scenario and results obtained are compared to evaluate the performance of each protocol. The Zigbee tests are performed using Memsic WSN kits. The WirelessHart tests are carried out using Emerson IWSN motes and the ISA-100 protocol tests are carried out by employing Yokogawa industrial motes. All these motes are widely used in industrial and experimental applications. The evaluation of each protocol is carried out to assess their performance in an industrial environment. Motes' power consumption and Received Signal Strength Intensity (RSSI) are the main parameters used for the evaluation of the protocols.

4.1 Protocols Experimental Tests

4.1.1 Zigbee Test

Zigbee is currently the oldest and most widely used WSN protocol. Many companies in the networking industry provide Zigbee-based products [14]. Memsic Inc. is one such manufacturers, whose devices can be used for conducting outdoor tests. These devices are able to sense voltage, humidity, temperature and pressure in a particular location. Their WSN kit provides an end-to-end enabling platform for the creation of wireless sensor networks. A windows application called MoteView is provided as an interface between the user and the deployed sensor network. MoteView also provides the tools to simplify deployment and monitoring. It also makes it easy to connect to a database, to analyze, and to graph sensor readings. In addition, it provides node health statistics in terms of transmission quality, number of dropped packets, number of retransmissions, etc.

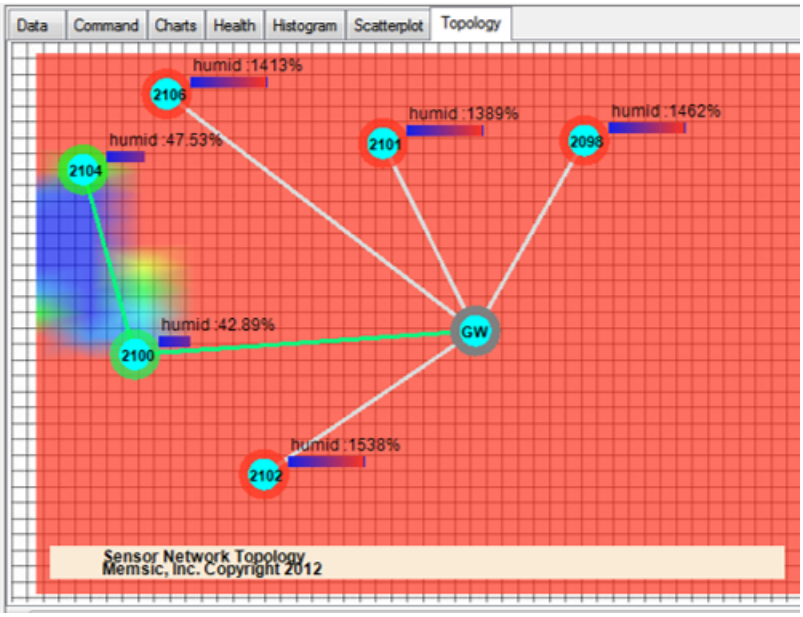


Figure 4.1: Topology for Humidity Measurements.

The topology for our experiment is shown in Figure 4.1. Devices numbered 2098, 2100, 2101, 2102, 2104 and 2106 as presented in Table4.1 act as sensor devices which sense humidity values and send them to a gateway device. Upon receiving the data, the gateway relays the received packets to a sink computer which displays the transmitted values in a GUI. Alarms are raised whenever there are some abrupt change(s) in some parameters being monitored. At the start of the test, packets started flowing from sensor devices to the gateway device at regular intervals.

We setup the network in an outdoor environment. We found the maximum transmission range from the node to the base station by powering just one node and moving it away from sink until the packets were not received (Figure 4.1). Node-to-sink maximum range was found to be about 80 m and node-to-node maximum range of transmission was found to be about 70 m.

We setup the nodes in a mesh topology as shown in Figure 4.1. We performed

Table 4.1: Drop in Battery Volts (Outdoor)

Drop in Battery Volts (V_d)				
Tx Period	0.3 sec	0.5 sec	1.0 sec	1.0 sec (40m)
Node	V_d	V_d	V_d	V_d
2098	0.03	0.02	0.01	0.01
2100	0.05	0.02	0.03	0.001
2101	0.02	0.02	0.01	0.01
2102	0.02	0.03	0.02	0.0002
2104	0.05	0.02	0.02	0.01
2106	0.02	0.03	0.01	0.01
Average	0.032	0.023	0.017	0.008

three experiments using different transmission periods (0.3 sec, 0.5 sec and 1.0 sec). For the second experiment, we kept the last data rate (1.0 sec) and changed the topology by moving nodes closer to each other and to the base-station by about half the initial distance. These values are manipulated for all nodes via the command tab on MoteView. We recorded the battery voltages of each node at the start and end of the experiment for each node. The drop in battery voltage is then calculated after each experiment. The energy consumed by each node is directly proportional to the square of this voltage-drop. Each experiment is run for an arbitrary time of about 20 minutes. Figure 4.2 shows a bar graph of the energy consumption per node calculated using the voltage drop for a transmission period of 1 sec, i.e. packets are transmitted every 1 sec.

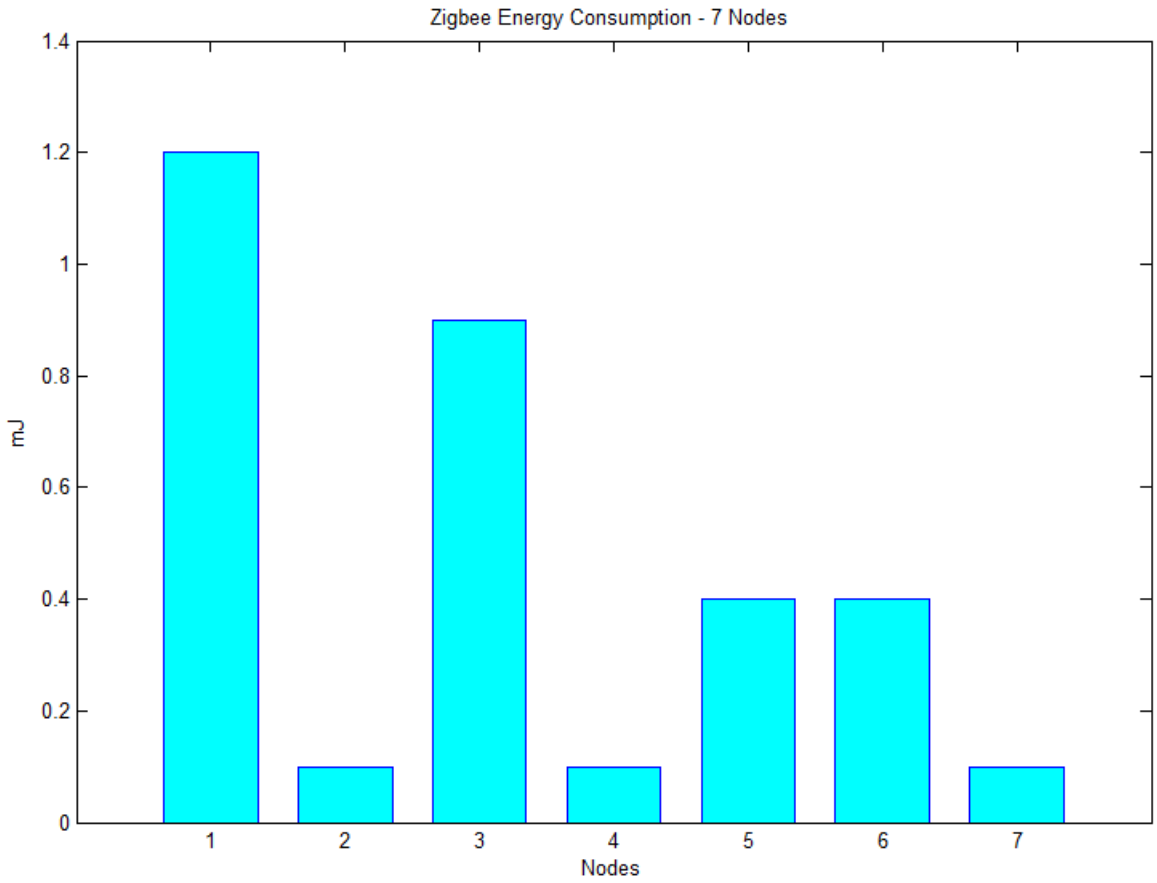


Figure 4.2: Energy Consumption per Node

As shown in Table 4.1, the average voltage drops in *volts* consumed by the nodes in the network for the four scenarios are 0.032, 0.023, 0.017 and 0.008 respectively as shown in the table. The battery voltages of the nodes are observed to decrease as the data transmission period is increased. This is due to the fact that, more energy is expended as the number of transmissions is increased in a certain transmission period. Further, it is observed that, the amount of power consumed is diminished by nearly half when nodes are moved closer to each other and to the base-station by about half the initial distance. This result indicate that Zigbee based wireless devices although consume minimal power will have limited application areas in the oil industry where instrumentation is done

across large distances. They could however be used in instrumenting compact indoor systems with minimal reliability and load requirements.

4.1.2 WirelessHART Test

Here, we present experimental work done to evaluate the WirelessHART protocol. This test is performed by employing Emerson devices, which operate using the WirelessHART standards. Like other devices, the kit consists of sensor and gateway devices, which serve to collect and transfer data. The topology used is shown in Fig. 4.3.

The testbed system for this protocol is composed of sensor nodes deployed in a mesh topology such that, when the setup is turned on, each device is able to connected to any other device in its range. The link configuration and stability according to the device tags is shown in Figure 4.3, which explains the link of gateway with the sensor nodes. It also shows the number of neighbor sensors of each network node. The reliability of the link and Received Signal Strength Intensity (RSSI) is also depicted.

Table 4.2: WirelessHART Device Tags and Description

Tag name	Description
385PI0501B	Pressure Transmitter model 3051S
385PI0211B	Pressure Transmitter model 3051S
385PI0026A	Pressure Transmitter model 3051S
385PI0701B	Pressure Transmitter model 3051S
385TI0806	Temperature Transmitter model 648T
385TI0807	Temperature Transmitter model 648T
1420 Wireless Gateway	Smart Wireless Gateway Model 1420

These experiments were conducted at King Fahd University of Petroleum and Minerals (KFUPM) stadium, in an outdoor environment on a sunny afternoon. The nodes were spaced 160m apart. Table 4.2 shows the device types and descriptions used in the experiments.

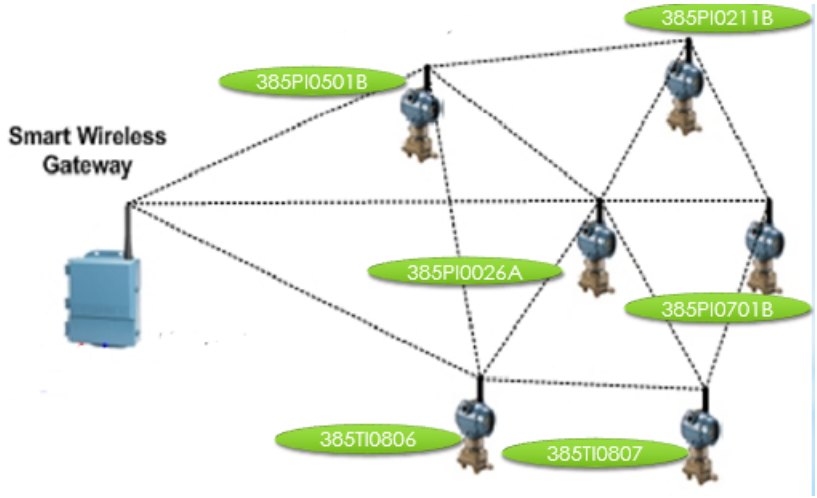


Figure 4.3: WirelessHART Test Topology

As shown in Figure 4.5, all 6 transmitters communicated to the Gateway with a high

communication reliability of greater than 99%. The communication reliability obtained from the Emerson WirelessHart kit is defined by emerson as the network throughput. A path stability of more than 97% was recorded for all nodes. Strong communication strength indicated by RSSI as shown in Figure 4.4 is observed to be well above -70dB for all nodes, which is a good indicator of strong SNR between each the WirelessHart network nodes and the basestation.

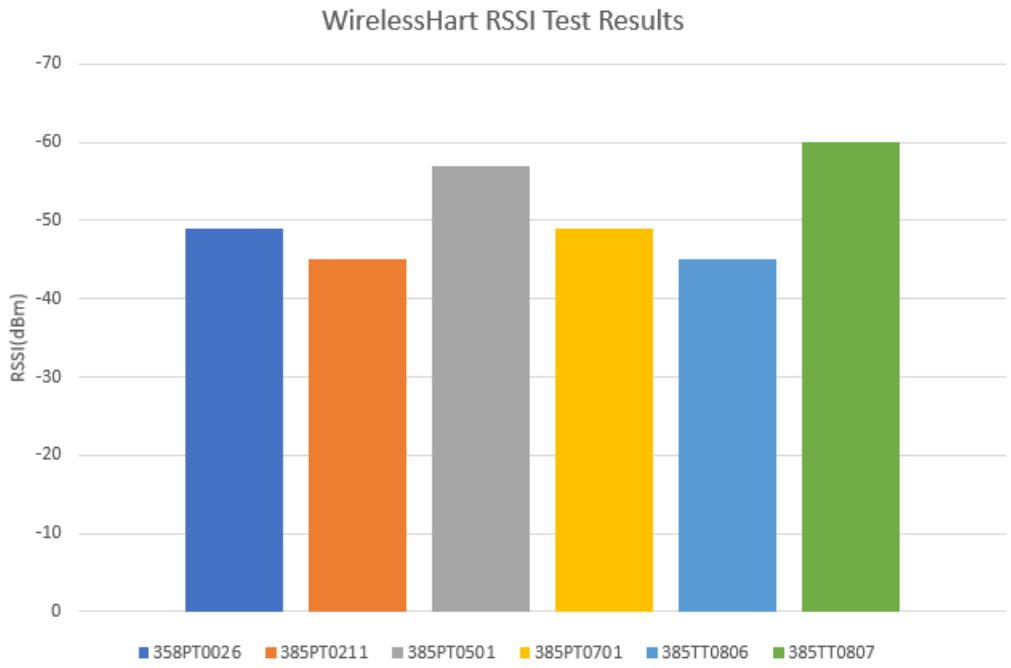


Figure 4.4: RSSI of Received Signal at Base Station

In Figure 4.5, the performance parameters for each node can be matched to its position in the topology. The said values mentioned above give a clear picture of how well the WirelessHart protocol operates in the field. The results obtained show that the Wireless Hart protocol performs well in outdoor conditions at distances of 200m and hence may be employed for instrumentation applications in the oil industry.

HART Tag	Node state	Active neighbors	Neighbors	Service denied	Reliability	Missed updates	Path stability	RSSI	Joins
385PT0026A		SFNY 385PT0701B 385PT0211B 385PT0501B	4		100.0 %	0	100.0 %	-49 db	1
385PT0211B		SFNY 385TT0806 385PT0026A 385PT0501B	4		100.0 %	0	100.0 %	-44 db	1
385PT0501B		SFNY 385PT0211B 385PT0026A	3		100.0 %	0	100.0 %	-57 db	1
385PT0701B		SFNY 385PT0026A	2		100.0 %	0	100.0 %	-49 db	1
385TT0806		SFNY 385PT0211B 385TT0807	3		100.0 %	0	100.0 %	-44 db	1
385TT0807		SFNY 385TT0806	2		100.0 %	0	97.0 %	-60 db	1

Figure 4.5: Wireless HART Test Performance Values

4.1.3 ISA100 Test

The purpose of this experiment is to find the appropriate range and terrain for the operation of IWSN in a typical industrial environment. Instruments used for testing are the Yokogawa wireless kit shown in Figure 4.6, which consist of field and gateway devices. If the path stability or reliability decreases as a result of any environmental change, the device will try to switch to an alternative path. The test was performed in two terrains, namely plane ground and rough ground (in which there are buildings and structures separating the field device from the gateway device). Two different environments are chosen so as to find the attenuation and signal degradation in the two surface cases.

Figure 4.6: Yokogawa Field Device Kit using 1SA 100.11a Protocol

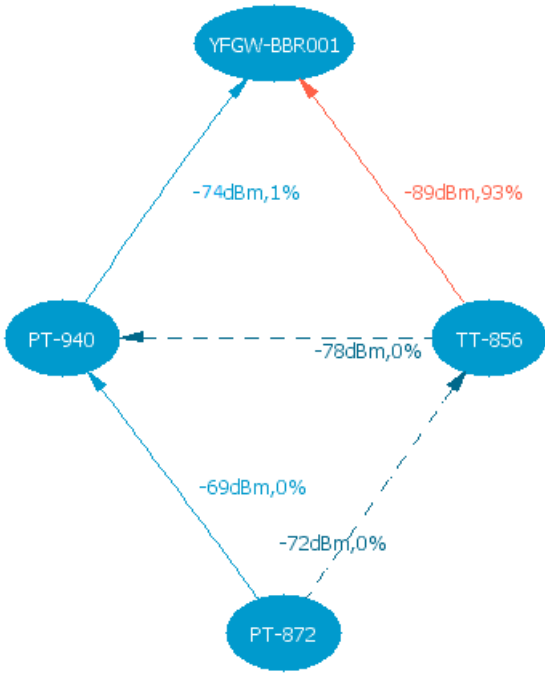


Figure 4.7: ISA 100.11a Test for Rough Surface.

These experiments were conducted at King Fahad University of Petroleum and Minerals (KFUPM) in an outdoor environment. Topologies used for this experiment for the

irregular and regular surfaces are shown in Figure 4.7 and Figure 4.8, respectively. A temperature sensor and two pressure sensors are used to sense the data and transfer it to the gateway device. Table 4.3 shows the device type and tags used.

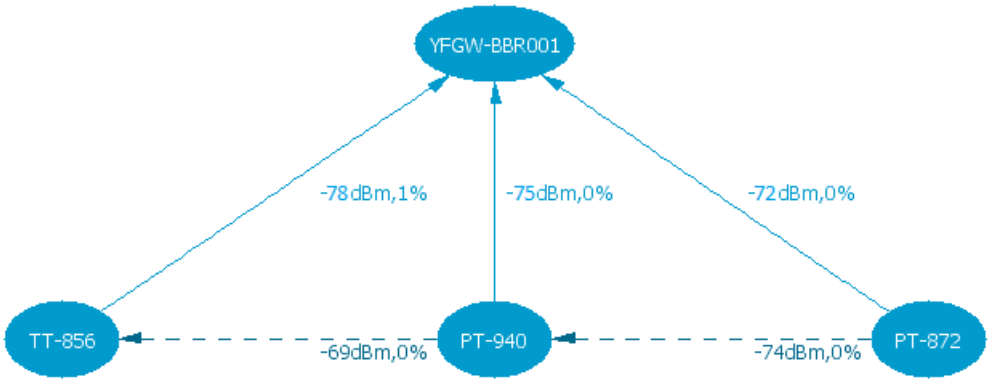


Figure 4.8: ISA 100.11a Test for Plane Surface

ISA100 takes into account the direct communication node and neighboring node for data transfer and in case one of the nodes goes down, it can automatically switch to another route based on the Packet Error Rate (PER) and RSSI. In the two topologies we have seen that the sensor devices are connected to the gateway device directly or indirectly. There are two kinds of connections shown in the topologies. Solid lines are actual communication routing between the device and gateway. Dotted lines are alternate routes which are used in case of fault or errors. For each link, the RSSI and PER as a percentage are indicated. In Figure 4.7, the device TT-856 was experiencing a higher PER while communicating to gateway device.

Table 4.3: ISA 100.11a Device Tags and Type

Device TAG	Functionality	Type
PT-872	IO Device +Router	Pressure Sensor
PT-940	IO Device +Router	Pressure Sensor
TT-856	IO Device +Router	Temperature Sensor
YFGW-BBR001	Gateway Device	Gateway Device

Table 4.4 shows the detailed statistics after collecting data from the two terrains.

Table 4.4: Network statistics collected from ISA test

Device TAG	Average Distance		Average RSSI (dBm)		Average PER (%) and Hop count	
	Flat Terrain	Rough Terrain	Flat Terrain	Rough Terrain	Flat Terrain	Rough Terrain
PT-872	600 m	1000 m	-72	-69	0 / 1	0 / 2
PT-940	600 m	600 m	-75	-74	0 / 1	1 /1
TT-856	600 m	1000 m	-78	-89 (-75)	0 / 1	93 / 1 (0.63/2)

To further evaluate the performance of ISA-100 in plane and rough terrains we compare the change in Received Signal Strengh Indicator (RSSI) values for these terrains. Figure 4.9 compares the RSSI values for the plane and rough terrains for the ISA-100 protocol.

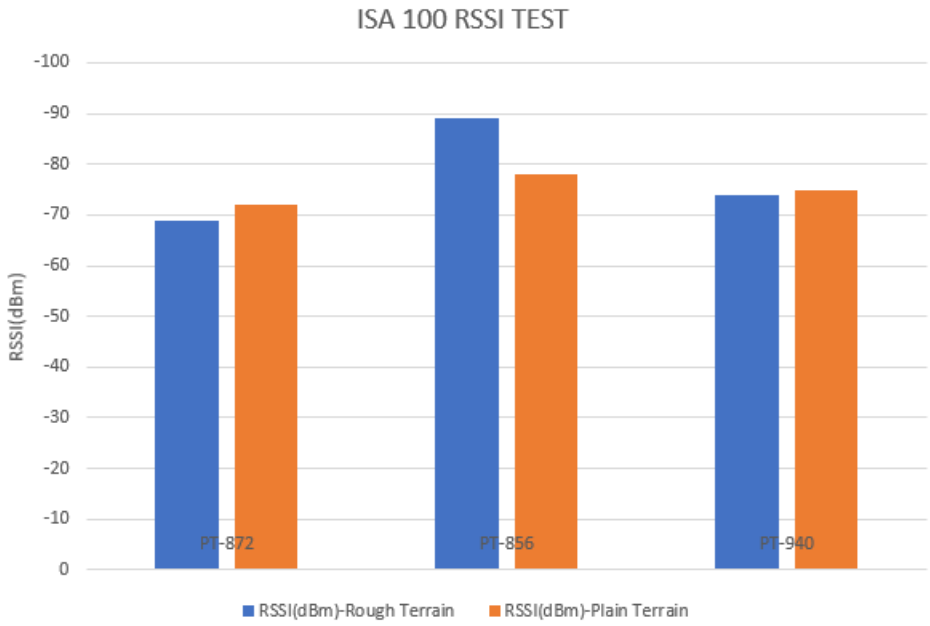


Figure 4.9: RSSI Comparison for Rough and Plain Terrains for ISA 100 Protocol

As shown in the graphs, the RSSI value of node PT-940 in the plane terrain is almost equal as compared to that of the rough terrain. For node PT-872, the RSSI value in the plane terrain is less as compared to that of the rough terrain. This is because, in the rough plane, this node chose an alternate path instead of the main path due to obstacles in the main path and hence retains a higher RSSI value. For node TT-856, the RSSI value in the plane terrain is higher as compared to that of the rough terrain. This is because the rough terrain communication through the direct link has a packet error rate of 93%, hence the alternate path with a low RSSI through node PT-940 is used. In the plane terrain however, node TT-856 communicate directly to the gateway with a much higher RSSI value.

4.2 Industrial Case-Study for ISA100.11a Evaluation

A practical experiment is performed in the Shedgum oil field in which IWSNs are deployed to instrument certain parameters of interest. The field and pressure sensors are installed in the test environment and all collected data are relayed to a base station located at a central control room. The experimental scenario is in accordance with Figures 4.10 which describe the sensors placed in different locations of Shedghum plant. All sensors nodes are programmed to sense the nearby data for temperature/pressure and send it to the central control room where the decision making is done based on the received data. Since the sensors cover the whole plant, they present an overall picture of the plant layout. For better decision making data should be error free and accurate. False data may lead to false alarms and may result in confusion amongst plant operators. The experiment is divided into practical and simulation, the results are than compared and concluded in the end.

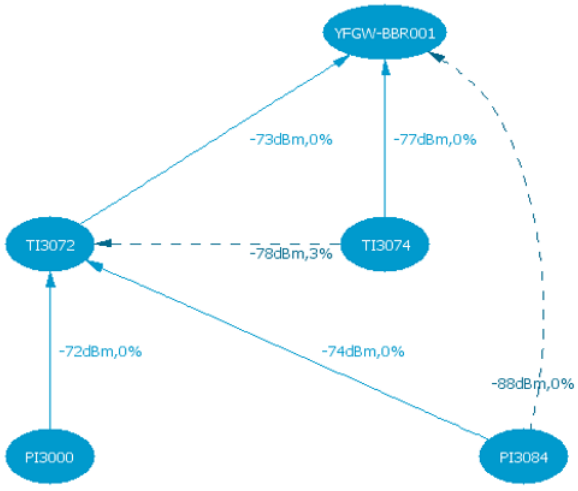


Figure 4.10: Experiment Topology Scenario in Shedgum Oil Field

1. The experiment was performed in Shedgum GOSP-3 plant, Shedgum, Saudi Arabia.

2. Yokogawas Field wireless System is used for conducting the experiment.

3. Temperature and pressure sensors are placed according to architecture shown in Figure 4.10. The purpose of these sensors is to collect temperature and pressure values from their designated places and forward it to Central Control Room (CCR).

4. The CCR collects all the data, analyze it, and raises alarms accordingly. Table 4.5 shows the sensors tags with their functionalities

5. A mesh topology illustrated in Figure 4.10 is used for this experiment .

6. Received Signal Strength Indicator (RSSI) and Packet Error Rate (PER) are calculated at CCR.

7. Each sensor generates 78 bits of data that is to be transmitted to CCR.

Table 4.5: Sensors and Gateway Descriptions

Model	Description	Quantity	Remarks
EJX110B	Wireless Pressure Transmitter	02	Tags: PI3000, PI3048
YTA510	Wireless Temperature Transmitter	03	Tags: TI3072, TI3073, TI3074
YFGW710	Wireless Gateway	01	.

4.2.1 Yokogawa Field Wireless System

This Yokogawa field wireless system is based on ISA100 and consist of two types of devices.

1. Wireless Field Device - Route Incoming Data

2. Wireless Field Gateway Device Collect data

Some of the field devices also act as input/output devices (IO). Some can act as router (i.e. they take data from IO devices and transmit it to CCR). The gateway device collects all the data from the field devices and sends it to CCR which is than displayed to the end user using application GUI. Neighbors in each case are determined which is shown is in the tables below. External noise was observed sometimes and very minimum interference was observed in the 2.4 GHz band.

4.2.2 Experiment

The RSSI and PER are calculated at the CCR. Field device TI3073 failed at the start of the experiment which can be seen at GUI of field wireless system. Yokogawa gateway R1.5 algorithm automatically created secondary path once it caught another device within the network. Primary paths were the routes used for data transfer to CCR. When there was noise or the primary link was unavailable, alternate routes were used, which were termed as secondary paths. RSSI and PER of each node from primary to secondary was taken at regular intervals. The received value was also compared with the actual value at the temperature and pressure sensor to check the integrity of the system. A very small difference in data was observed showing that the system could be trusted. Table 4.6 and Table 4.7 show the received RSSI and PER for primary and secondary paths.

Yokogawa has established the criteria for reliable wireless communication using Yokogawas ISA100.11a field wireless devices. Since RSSI accuracy depends on the RF chip from each vender and RSSI criteria depends on RF chips minimum receive sensitivity,

Table 4.6: RSSI and PER on Primary route

Device Tag	Neighbor Tag	RSSI [dBm]	PER[%]	Error	Success
PI3000	TI3072	-72	0.018	539	2,931,693
PI3084	TI3072	-74	0.0073	21	2,865,621
TI3072	YFGW-BBR001	-73	0.0106	696	6,550,851
TI3074	YFGW-BBR001	-77	0.234	3,614	1,541,188

Table 4.7: RSSI and PER on Secondary route

Device Tag	Neighbor Tag	RSSI [dBm]	PER[%]	Error	Success
PI3000	-	-	-	-	-
PI3084	YFGW-BBR001	-88	0.33	706	212,342
TI3072	-	-	-	-	-
TI3074	TI3072	-78	3.7	6,592	167,079

Yokogawa has selected PER as the criteria. If the PER is more than 15%, Yokogawa wireless system identifies that the LOS is not secured and recovers the packet loss by using retry slot of transmission, or alternate route [15].

It is observed that for the primary route the RSSI for all nodes ranged between -77dB to -72dB. The packet error rate on the other hand was below 0.1 % for all nodes. This results indicate that, the ISA-100 protocol performed excellent in the said experimental scenario. As shown in Table 4.7, results obtained through the secondary routes also fall below the 15% accepted PER specified by Yokogawa.

It is observed here that the secondary route can be used in case of network congestion or failed transmission scenarios. A packet may be transferred to the gateway in more

Table 4.8: Temperature at regular interval of experiment

Range (%)	Simulated Value (F)	Measured Value (F)	Difference (%)
0	0.0	0.0	0%
25	50.0	50.2	0.40%
50	100.0	100.0	0%
75	150.0	149.9	-0.07%
100	200.0	200.0	0%

Table 4.9: Pressure at regular intervals of Experiment

Range (%)	Simulated Value (psi)	Measured Value (psi)	Difference (%)
0	0	0.0283	X
25	75	75.7485	0.99%
50	150	144.5691	-3.76%
75	225	220.4601	-2.06%
100	300	301.4550	0.48%

than 1 hop. Number of hops is decided based on the network parameters. Since the temperature and pressure sensors are used, another challenge is to check the data integrity and reliability of the system. It is important to check whether the value received are actual values or not. For this the field devices are monitored for time and values of the pressure and temperature are compared at regular intervals of experiment in order to get the actual difference. Tables 4.8 and 4.9 depict the experimental and simulation values and their respective percentage differences for temperature and pressure measurements respectively. The percentage disparity between experimental and simulation results are observed to be below ±0.5% for temperature measurements and below ±4.0% for pressure measurements.

The RSSI values of the experimental work is compared with simulation results obtained using a modeled Yokogawa simulator. Figure 4.11 presents graphs of this comparison. Since the deployment of IWSN takes a lot of resources and expertise, simulations are normally carried out to obtain expected Received Signal Strength Indicator(RSSI) and other performance parameters (not considered in this thesis) before real time deployment is carried out. The actual obtained field RSSI values are observed here to be relatively close to the expected RSSI values.

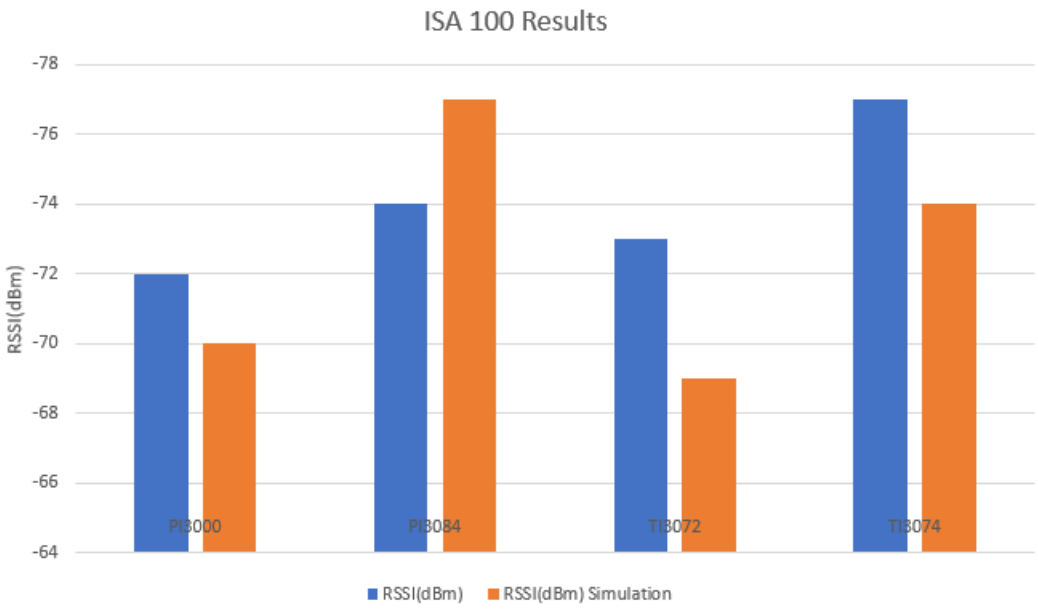


Figure 4.11: Experimental and Simulation Results Comparison

To conclude, in this chapter, we have studied and conducted the lab test of Zigbee, WirelessHART and ISA100. The results are compared and analyzed in order to evaluate the best protocol for IWSNs. The Yokogawa field wireless kit offers a far better range that is greater than 800 meters, which is suitable for bigger industries and cuts the cost of additional gateway devices used to connect all the edges in a factory. The WirelessHART protocol then follows in performance in terms of application range and cost. The Zigbee protocol however has a limited range of application and hence is good for indoor and experimental applications.

CHAPTER 5

SIMULATION OF IWSN

5.1 Introduction

Wireless Sensor Networks (WSNs) have been employed in many important applications such as intrusion detection, object tracking, industrial/home automation, smart structures and several others. The development of a WSN system requires that the design concepts be first checked and optimized using simulation [16].

The simulation environment for WSNs can either be an adaptive development or a new development. The adaptive development includes simulation environments that already existed before the idea of WSNs emerged. These simulation environments were then extended to support wireless functionality and adapted for use with WSNs. In contrast, new developments cover new simulators, which were created solely for simulating WSNs, considering sensor specific characteristics from the beginning [17]. Recently, several simulation tools have appeared to specifically address WSNs such as NS3, Cooja and Castalia [18], varying from extensions of existing tools to application-specific simulators.

Although these tools have some collective objectives, they obviously differ in design goals, architecture, and applications abstraction level [16].

Simulators can be divided into three major categories based on the level of complexity:

- algorithm level,
- packet level, and
- instruction level.

Some algorithm-level simulators are described in [19], [20], [21] and [22].

Simulation has always been very popular among network-related research. Several simulators have been developed to implement and study algorithms for wireless networks. Some are general-purpose while others are designed for a specific purpose and vary in features and level of complexity. They support certain hardware and communication layers assumptions, and provide a set of tools for deployment scenarios, modeling, analysis, and visualization. Classical simulation tools include NS-2/3, OPNET, OMNeT++, J-Sim, and TOSSIM [17][23][18].

5.1.1 OMNeT++

OMNeT++ is a discrete event simulation environment. Its primary application area is the simulation of communication networks, but because of its generic and flexible architecture, it is successfully used in other areas like the simulation of complex IT systems, queuing networks or hardware architectures as well [24][25].

OMNeT++ provides a component architecture for models. Components (modules) are programmed in C++, then assembled into larger components and models using a

high-level language (NED). Reusability of models comes for free. OMNeT++ has extensive GUI support, and due to its modular architecture, the simulation kernel (and models) can be embedded easily into applications. Although OMNeT++ is not a network simulator itself, it is currently gaining widespread popularity as a network simulation platform in the scientific community as well as in industrial settings, and building up a large user community [15].

5.1.2 Castalia

The intended simulation platform is Castalia which is a simulator for Wireless Sensor Networks (WSN), Body Area Networks (BAN) and generally networks of low-power embedded devices [18]. It is based on the OMNeT++ platform and can be used by researchers and developers who want to test their distributed algorithms and/or protocols in realistic wireless channel and radio models, with a realistic node behavior especially relating to access of the radio. Castalia can also be used to evaluate different platform characteristics for specific applications, since it is highly parametric, and can simulate a wide range of platforms. The main features of Castalia are:

1. Advanced channel model based on empirically measured data.

2. Advanced radio model based on real radios for low-power communication

3. Extended sensing modeling provisions

4. Node clock drift, CPU power consumption.

5. MAC and routing protocols

6. Designed for adaptation and expansion.

5.1.3 Pymote

After some research, we concluded that Python-based tools completely fulfill our requirements. We decided to use Pymote [26], which is a high level Python library specifically designed for wireless networks to perform event based simulation of distributed algorithms. Users can implement their ideas in Python; which has become popular in academia and industry. The library is developed without much abstraction and therefore can be used or extended using Python's highly expressive native syntax. The library particularly focuses on fast and accurate implementation of ideas at algorithm level using formally defined distributed computing environment.

In this work, we use extended Pymote, which is a high level open source Python library for event based simulation of distributed algorithms in wireless ad-hoc networks, for generating topologies. After one year of extension and development, the framework is completed and ready to perform interactive simulation [27]. We implemented graphing and data collection modules to enhance the Pymote base functionality and modified existing modules for node, network, algorithm, simulation and logging to support the extended framework [28]. The extended framework utilizes the python Matplotlib package [29] and the innovative charting library provided by Highsoft [30], which is free to use for personal and academic purposes. The output format includes CSV, PNG, and high quality SVG and PDF which can directly be inserted into Latex and other publishing applications. HTML files are also created with embedded JavaScript for interactive plot-

ting which is needed for presentations and on-line content. Following is a simple python script for simulating 'Flood' message among few nodes using Pymote. Figure 5.1 shows the corresponding generated topology.

```
1  from pymote import *
2  net_gen = NetworkGenerator(degree=2, n_count=19)
3  #net = net_gen.generate_random_network()
4  #net = net_gen.generate_neigborhood_network()
5  net = net_gen.generate_homogeneous_network()
6  from pymote.algorithms.broadcast import Flood
7  net.algorithms = ( (Flood, {'informationKey':'I'}), )
8  some_node = net.nodes()[0]
9  some_node.memory['I'] = 'Register'
10 sim = Simulation(net)
11 sim.run()
12 net.savefig(fname=__name__)
```

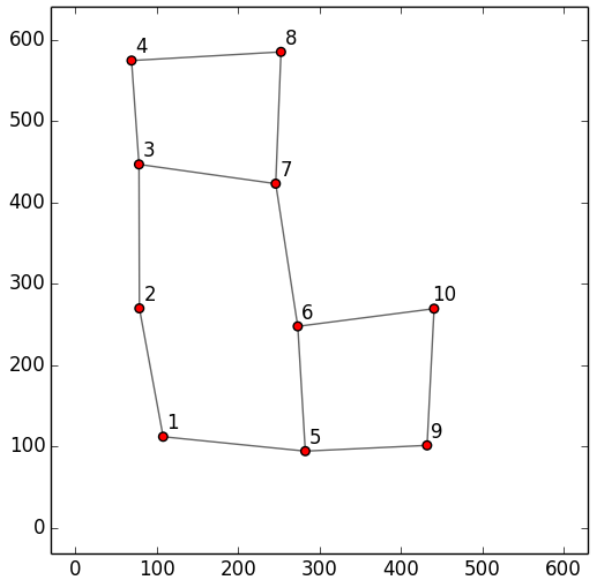


Figure 5.1: A 10-nodes WSN topology using Pymote

5.2 Simulation Framework

5.2.1 Propagation model

For this work, we use the shadowing model, where the received power is a random variable due to multi-path propagation or fading (shadowing) effects. The shadowing model consists of two parts: path loss component and a Gaussian random variable with zero mean and standard deviation σ_{DB}, which represents the variation of the received power at certain distance. Table 5.1 lists parameters available for the propagation module.

Table 5.1: Propagation model Parameters

Description	**Parameter**	**Default**
System Loss (>=1.0)	L	1
Min. Received signal power threshold	P_RX_THRESHOLD	-70 dbm
Frequency	FREQ	2.4 Ghz
Path loss exponent	BETA	2.5
Gaussian noise standard deviation	DB	4 dbm
Transmit Power	P_{Tx}	0.084 W

5.2.2 Error Model

Bit error rate (BER) is commonly used for evaluating the performance of wireless devices. BER is measured by checking which bits are received incorrectly during the communication of predetermined bit patterns. This requires a dedicated program in the devices, and

needs considerable amount of processing. On the other hand, packet error rate (PER) is the ratio of incorrectly received packets to the whole packets transmitted. This measurement can be done without any special tools, and therefore most commonly used for evaluation of wireless communication in real environment. We use the Gilbert/Elliot error model [8].

5.2.3 Energy Consumption Model

In our extended framework, the energy model object is implemented as a node attribute, which represents the level of energy in a node. The energy in a node has an initial value which is the level of energy the node has at the beginning of the simulation. It also has a given energy consumption for every packet it transmits and receives which is a function of packet size, transmission rate and transmit (receive) power. The model also supports idle or constant energy discharge due to hardware/micro-controller consumption. During simulation, each nodes available energy is recomputed every second based on the discharging rate. If it drops below minimum energy required to operate (E_{min}) then that node is assumed to be dead (not available for communication). The energy object keeps track of the energy available and total energy consumption. The parameters are set based on the target WSN system or protocol. The overall energy consumption of a node n is given by:

$$Energy(n) = P_{TX}.t_{TX} + P_{RX}.t_{RX} + P_{Idle}.t_{Idle}$$

Where P_{TX}, P_{RX} and P_{Idle} are the power consumed is transmission, reception and when idle respectively

5.3 Simulation of IWSN

For all our simulations, first we used topology generator module to generate the appropriate topology for each type of protocol. Then, we employed the Castalia framework to carry out the simulations and collect several statistics. The results are analyzed statistically and visually using interactive charts and plots on Pymote extended framework.

In our work, the performance metrics considered are;

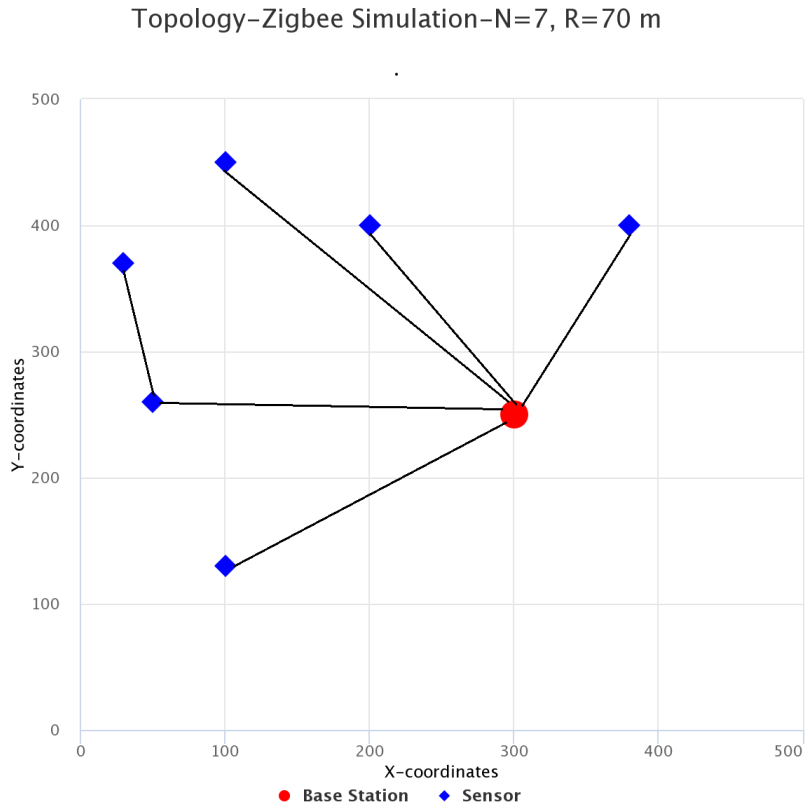
1. Communication cost per Node, in terms of number of packets transmitted, lost and received during a simulation run.

2. Energy Consumption, which is proportional to the communication cost and size of the packet.

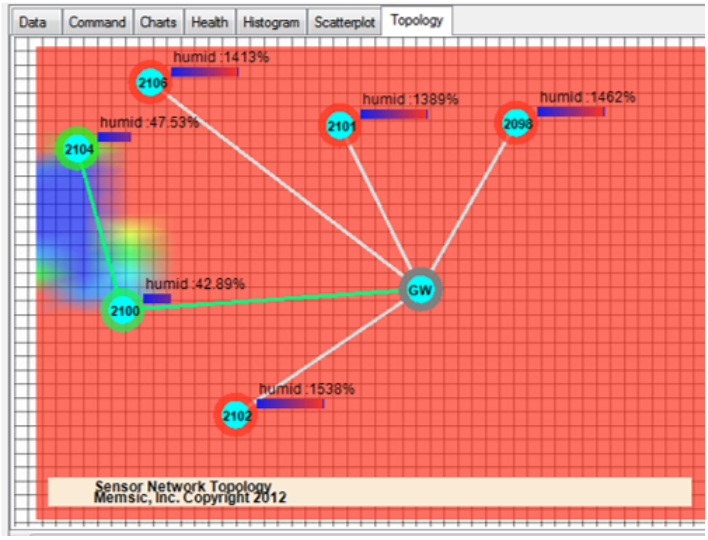
5.3.1 Simulation Setup

For our simulation, nodes are deployed in a 500m x 500m area. We have three separate simulation script for three protocols which are configured with appropriate parameters. We used similar node layout as we have for the experiments, as described in chapter 4. Figures 5.2 to 5.5 show the three topologies showing the base station with a bigger marked circle or square.

The number of nodes and communication range (R) are shown on top of each figure.



(a) Simulation



(b) Practical

Figure 5.2: Topology for Zigbee Simulation

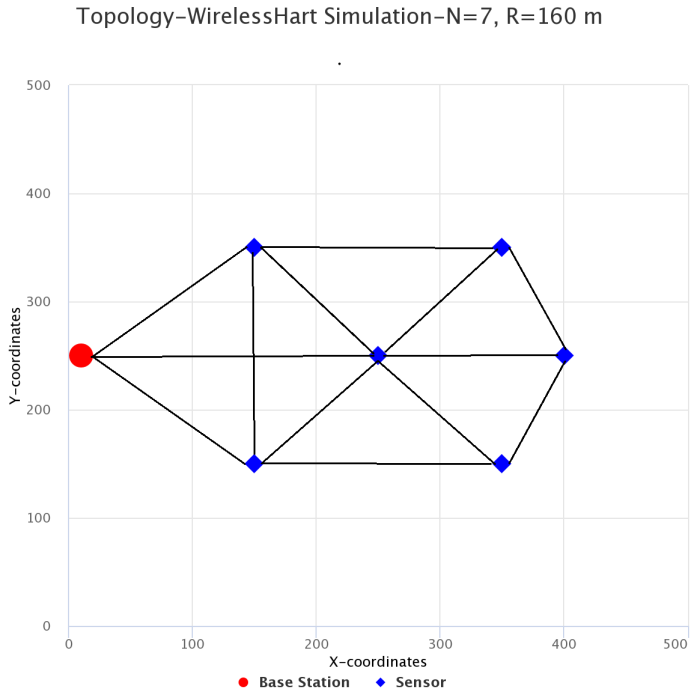
Figure 5.2 shows the topology for Zigbee simulation with bigger square representing sink node. Figure 5.3 shows the topology for WirelessHART simulation making a mesh network with 7 nodes. Finally, Figure 5.4 and 5.5 show the topologies employed for the ISA 100 simulation. For ISA 100, we simulate two scenarios or terrains, namely plain ground (no obstacle) and Rough ground (in which there are obstacles due to buildings and structures separating the field device from the gateway device). This option of a rough terrain with obstacles is found in the Pymote simulator module.

5.3.2 Simulation Description

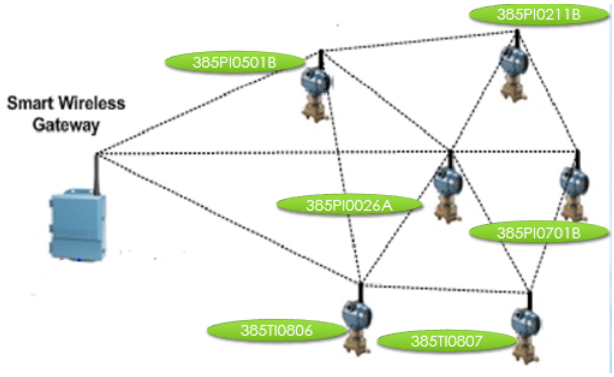
At the beginning of simulation, the base station sends the beacon or a registration message to all nodes. This allows nodes to transmit data packets to base station and simulation will terminate when Max_{Packet} (settable parameter) number of packets are transmitted [31]. We consider registration and data packet sizes of 90 bytes while the acknowledgment packet size is 15 bytes. During the simulation, the script keeps track of the number of transmissions, reception and lost packets. The energy consumption at each node is also computed dynamically.

5.3.3 Simulation Results

Due to constraints in both practical experiments and simulation tools, we couldn't obtain exact performance values of the practical experiment in our simulations, rather we generate results which relate to those obtained in the practical results. For zigbee, we generate energy consumption values to compare with values obtained practically. However, energy

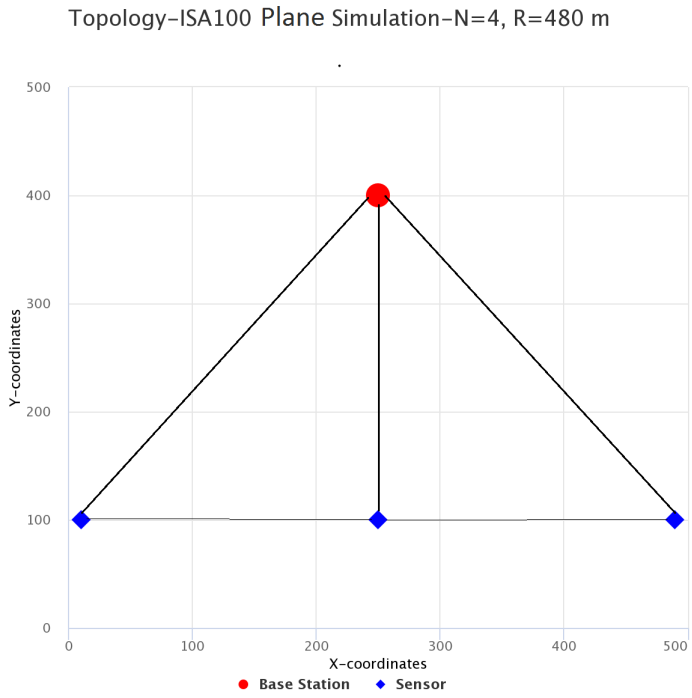


(a) Simulation

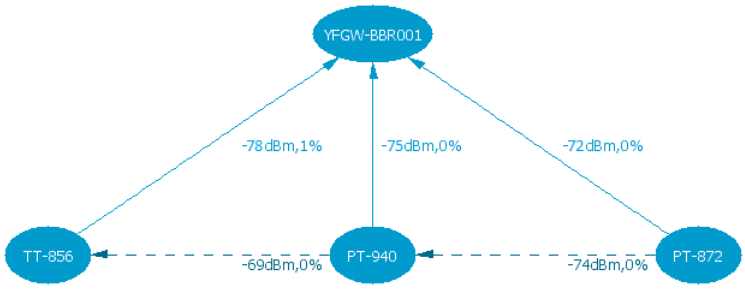


(b) Practical

Figure 5.3: Topology for WirelessHart Simulation

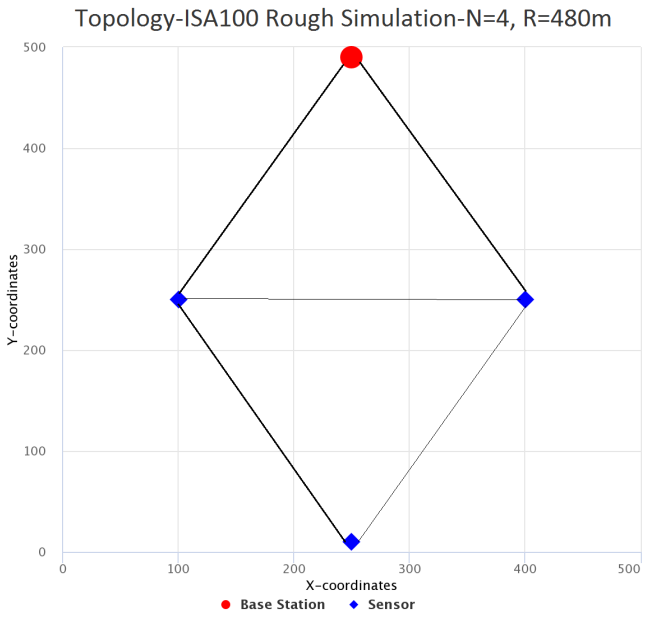


(a) Simulation

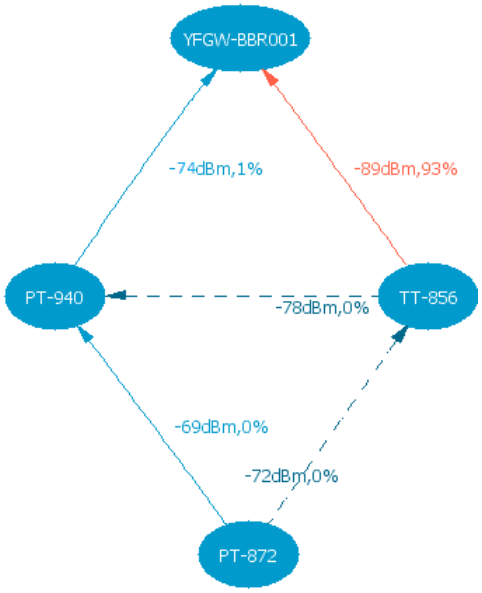


(b) Practical

Figure 5.4: Topology for ISA-100.11a Simulation in Plane Terrain



(a) Simulation



(b) Practical

Figure 5.5: Topology for ISA-100.11a Simulation in a Rough Terrain

consumption could not be obtained practically for WirelessHart and ISA-100.11a but results for these metrics are generated for the simulation to generally get a sense of the performance of these protocols for the practical topologies adopted. Packet Error Rate values which are practically generated for ISA-100.11a could however be compared to the simulation results of Packet Loss. PER represents the percentage of packets received with errors, at the base station. The metric which is also dubbed Throughput, S gives a measure of the percentage of successfully transmitted packets. This is the opposite of Packet Error Rate(PER), i.e., $PER = 1 - S$.

Figure 5.6 shows the energy consumption per node in milli-Joules (mJ) for Zigbee

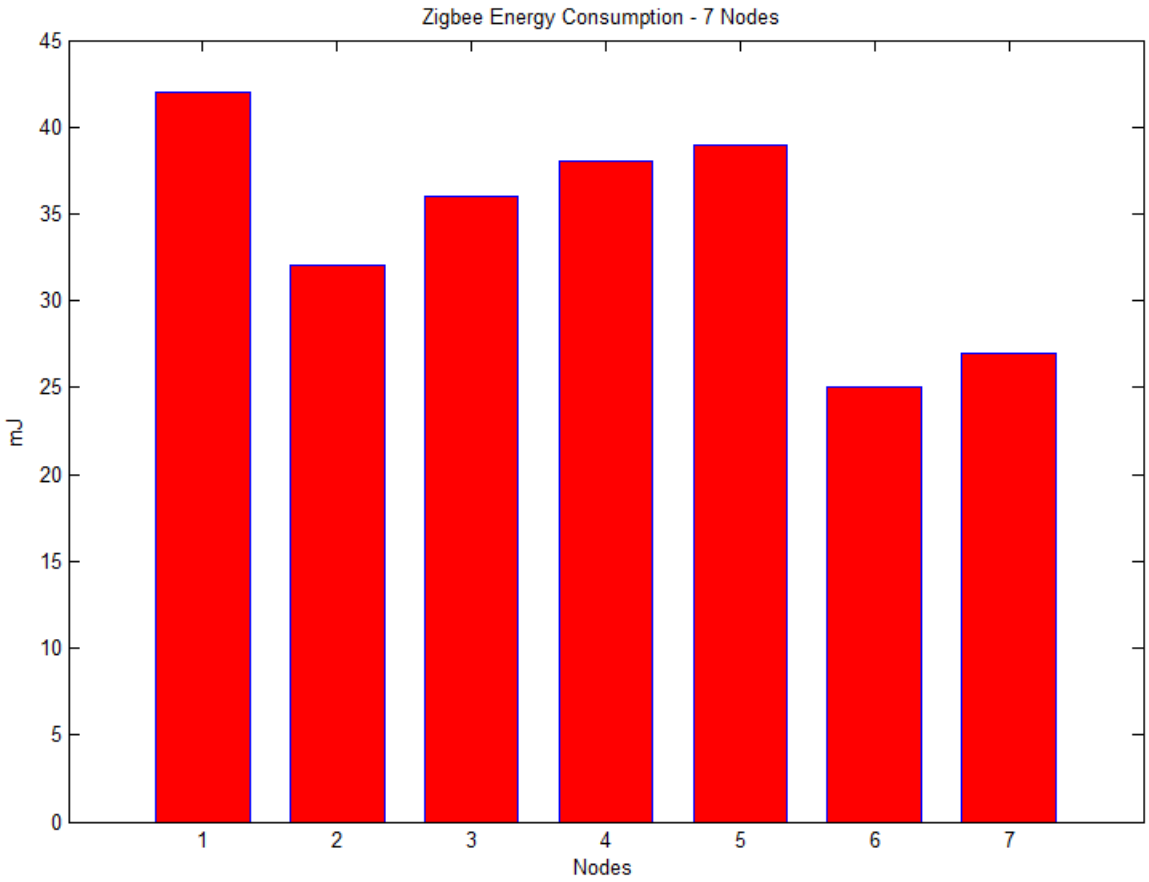


Figure 5.6: Energy Consumption per node for Zigbee Simulation

simulation (for all 7 nodes). The base station (node 1) has most power consumption as it is receiving packets from all other nodes (receiving power plus transmit power for message acknowledgment). In general however, the amount of power consumed in transmission is higher than that consumed in reception. Also node 4 and 5 have higher consumption as they are acting as relay nodes. This results is collaborated by the practical energy consumption results (Refer to Figure 4.2).

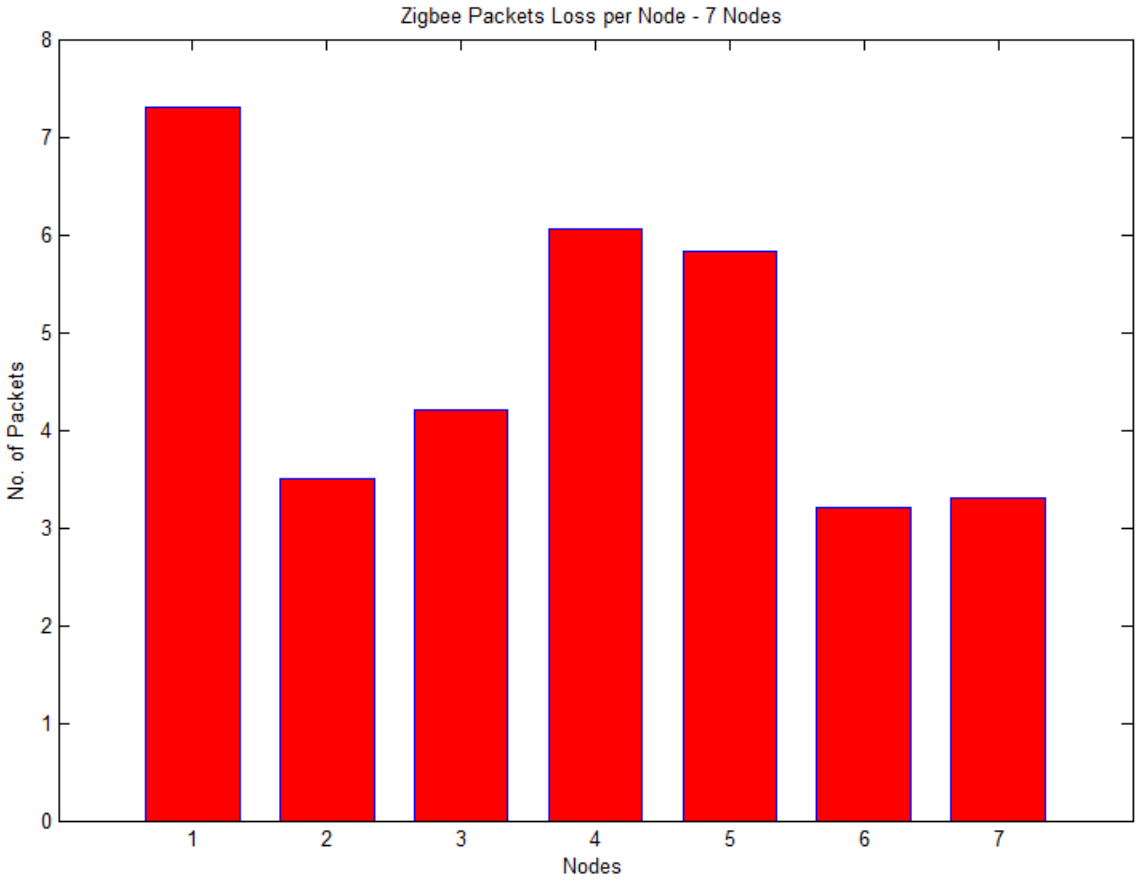


Figure 5.7: Packet Loss per Node for Zigbee Simulation

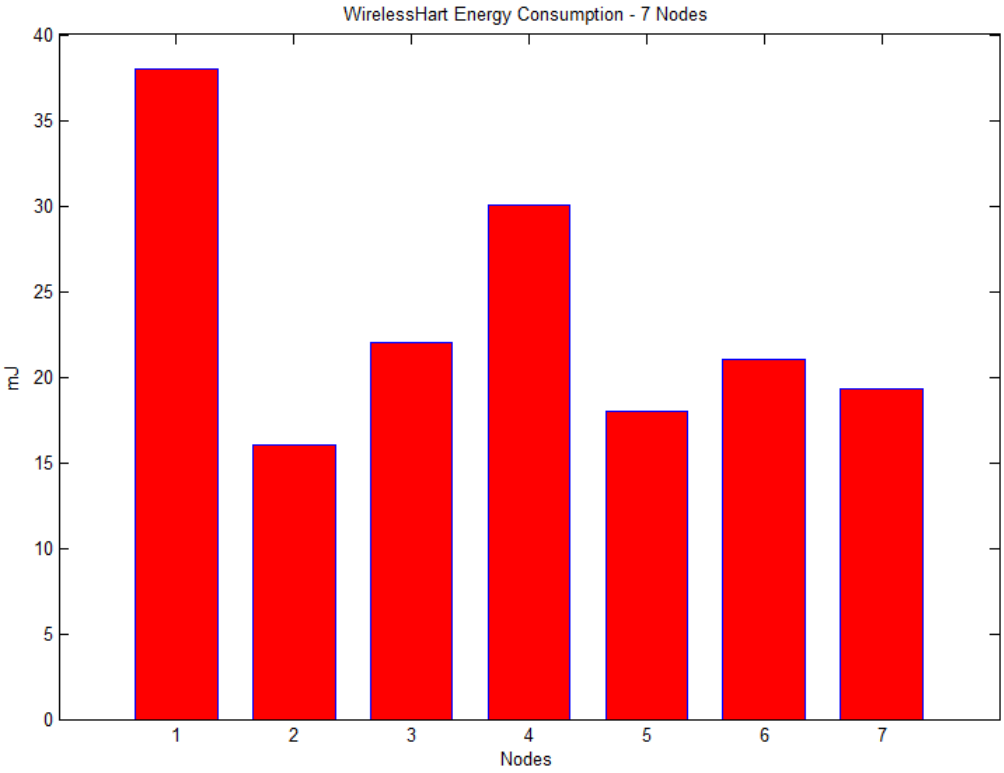


Figure 5.8: Energy Consumption per Node for WirelessHart Simulation

Fig. 5.7 shows the packet loss at receiver of each node based on the selected PER. Again nodes 1 and 4 have higher value as many packets are received by these nodes. Similarly, Figure 5.8 shows the energy consumption per node for WirelessHART simulation. The center node (node 3) has most power consumption as it is receiving packets from all other nodes. Fig. 5.9 shows the packet loss at receiver of each node based on the selected PER for WirelessHart. Node 7 has higher value as it is always communicating over multi-hop with the base station.

We see a high energy consumption for node 3 because it is located at the center of the network and hence is used as a relay node by most of the nodes to reach the base-station. Also this node experiences a high number of lost packets. This might be due to congestion resulting from the intermediary role this node serves. The last three

nodes (5,6 and 7) consume almost the same energy since they are all a distance from the base-station and therefore expend more energy in transmitting to the base-station. Node 7 however experiences the highest packet loss since its the furthest from the base-station.

Figure 5.10 shows the energy consumption per node for ISA100.11a simulation in a rough terrain. The energy consumption is fairly evenly distributed among nodes. As seen for the other protocols, the base-station consumes the most energy. Nodes 2 and 4 consumes almost the same energy but node 3 consumes more since it is sometimes used as a relay to reach the base-station.

Figure 5.11 shows the packet loss at receiver of each node. The base station (node

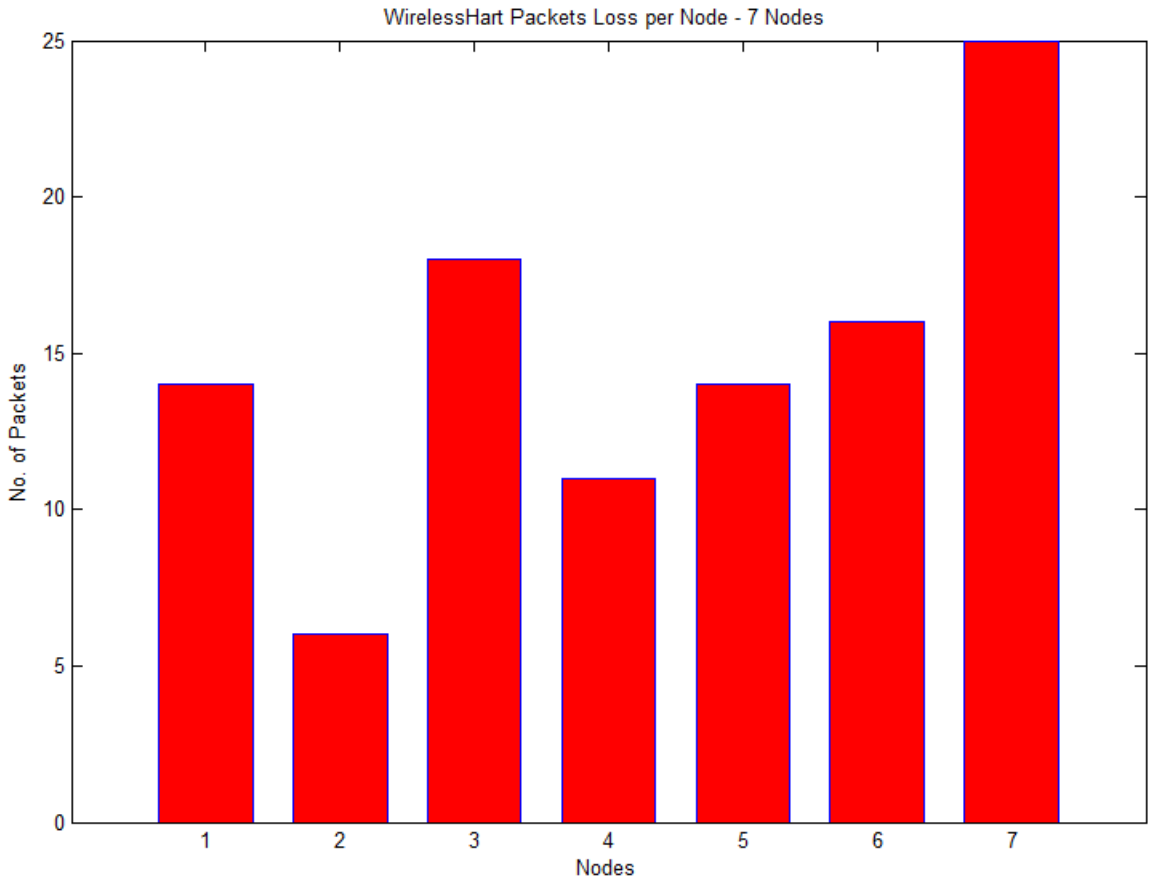


Figure 5.9: Packet Loss per Node for WirelessHart Simulation

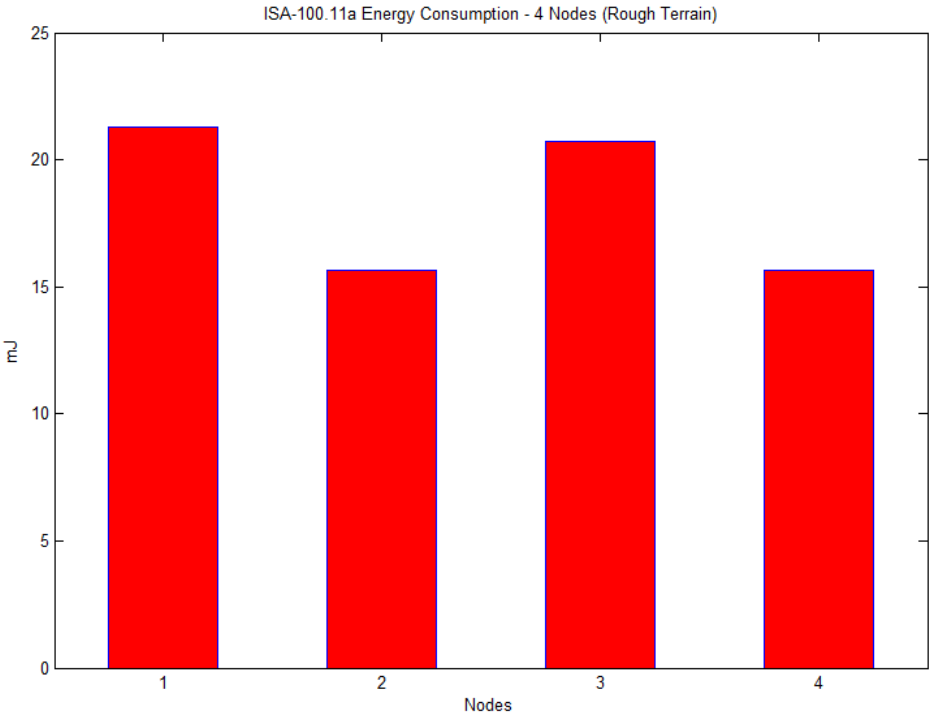


Figure 5.10: Energy Consumption per Node for ISA100.11a Simulation

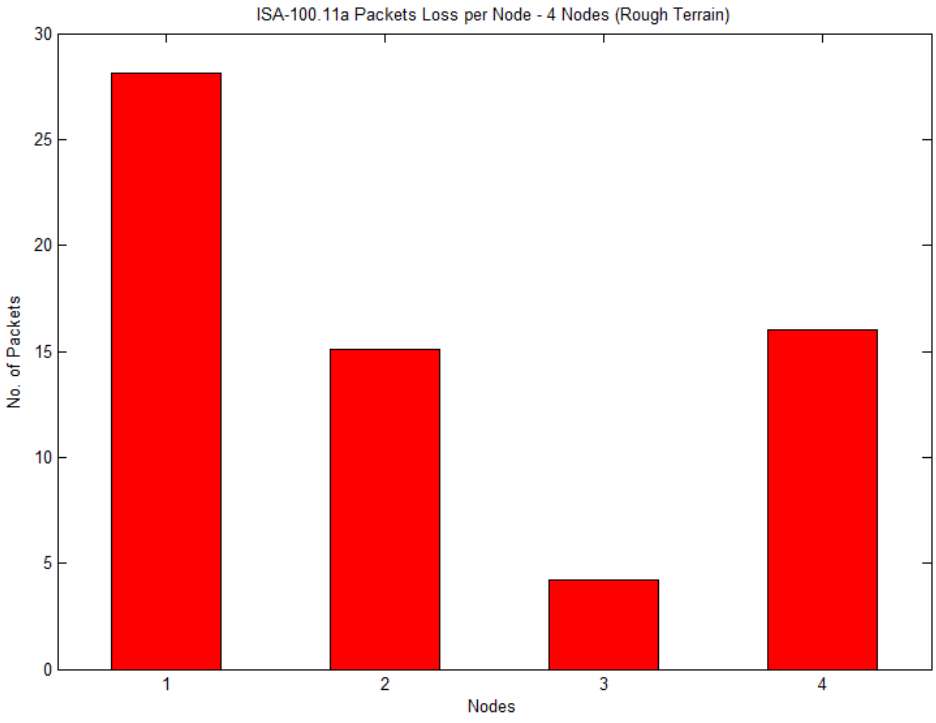


Figure 5.11: Packet Loss per Node for ISA100.11a Simulation

1) has higher value as it is receiving most packets. The practical results showed node 4 with higher PER although its packet loss values are less in the simulation. Node 3 has much lower value which is similar to the pattern in the practical results.

Figure 5.12 shows the energy consumption per node for ISA100.11a simulation in a plane terrain. The energy consumption is fairly evenly distributed among nodes. As seen for the other protocols, the base-station consumes the most energy. Nodes 2 and 4 consumes almost the same energy but node 3 consumes more since it is sometimes used as a relay to reach the base-station.

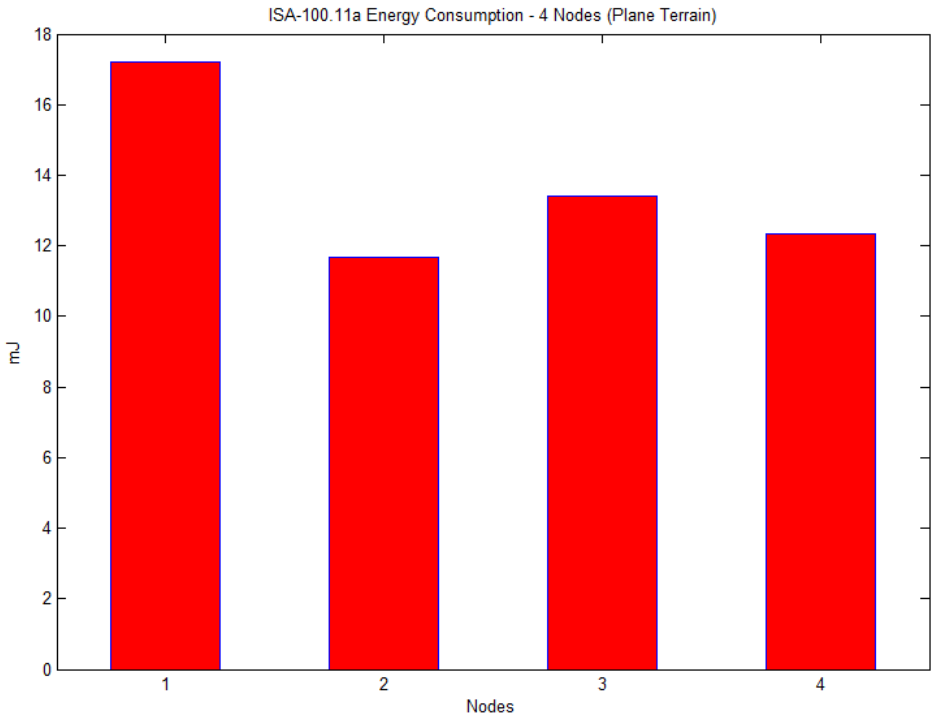


Figure 5.12: Energy Consumption per Node for ISA100.11a Simulation

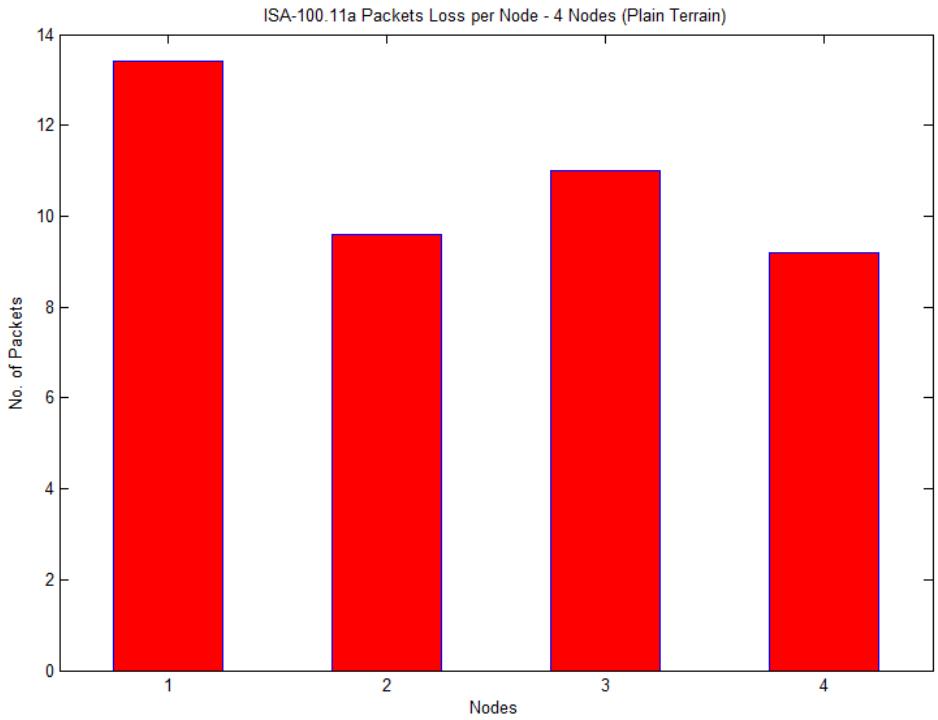


Figure 5.13: Packet Loss per Node for ISA100.11a Simulation

Fig. 5.13 shows the packet loss at receiver of each node. The base station (node 1) has higher value as it is receiving most packets. Nodes 2 and 4 are observed to have similar values with node 3 having a slightly larger value which in turn is less than the number of losses at the base-station. A similar pattern of the energy consumption is observed here for the rest of the nodes. We observe that energy consumption and packet loss of all nodes here are less relative to the simulation values in the rough terrain. This might be due to the fact that in this terrain, there's a line of sight for nodes to reach their respective destinations.

Hence it can be inferred from the above results that for the same packet payload, ISA-100 consumes the least power while communication over longer distances as compared to Zigbee and WirelessHart but prone to more packet losses as compared to these protocols.

5.3.4 Unified Simulation Configuration

To get more insight on the performance of the 3 protocols, a unified simulation configuration is tested. For this simulation, we employed the same network topology for all three protocols. Nodes are deployed in a 2000m x 2000m area. We used pymote for this simulation with three separate simulation scripts for each protocol. The number of packet transmissions for each simulation run was set to 2000. We utilized a 20 node network configured in a random topology for the evaluation of all protocols with one node acting as the gateway or base station.

Thus three simulation runs are carried out one for each protocol. In each topology we generate results for energy consumption and lost packets per node measured between each node and the base station. The base station is deployed in the middle of the network. Figures 5.14, 5.15 and 5.16 shows the adopted topology for ISA 100.11a, WirelessHart and Zigbee protocols respectively with the most probable links through which communication take place based on the transmission range of each protocol. The gateway node is designated as a bigger node in the center of the network labeled G. This same network layout is adopted for all protocols but a maximum transmission range of 500m, 200m and 150m are used for ISA 100.11a, WirelessHart and Zigbee protocols respectively. Since these transmission ranges are near each protocols' respective capacity, it is assumed that results obtained for the same network topology could be used to compare the performance of these protocols. Results obtained for the simulation are observed to see the pattern of energy consumption and packet reception efficiency for each protocol. We then make inferences based on the observed patterns. It should be

mentioned that, the mathematical/analytical descriptions of these protocols is beyond the scope of this thesis.

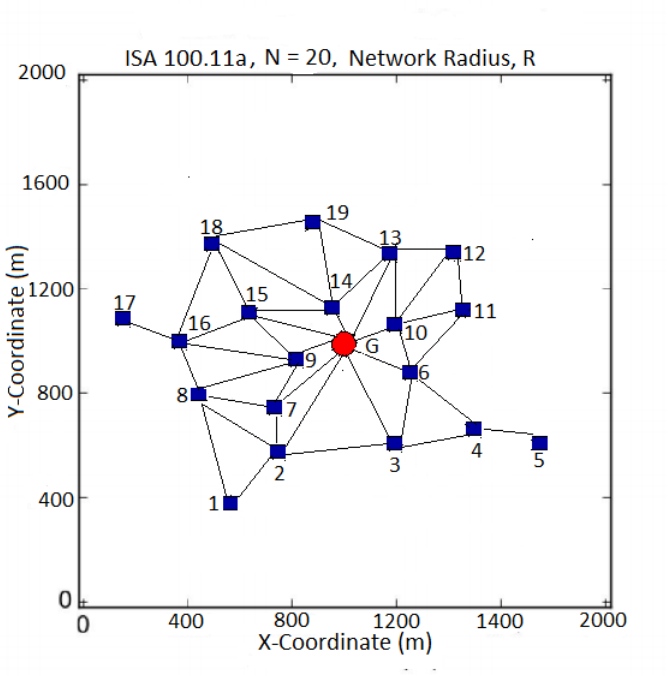


Figure 5.14: 20 Node Random Test Topology for ISA 100.11a Protocol

5.3.4.1 Energy Consumption Comparison

Figure 5.17 show the energy consumption of each network node in *milliJoules* for Zigbee, WirelessHart and ISA 100.11a protocols. It is observed here that the energy expended by all nodes for the three protocols fall below $122mJ$. As shown in Figure 5.17 the base station node was observed to consume the most energy for all protocols but as expected for the same network layout and conditions, ISA 100.11a consumes less than WirelessHart which in-turn consumes relatively less than Zigbee.

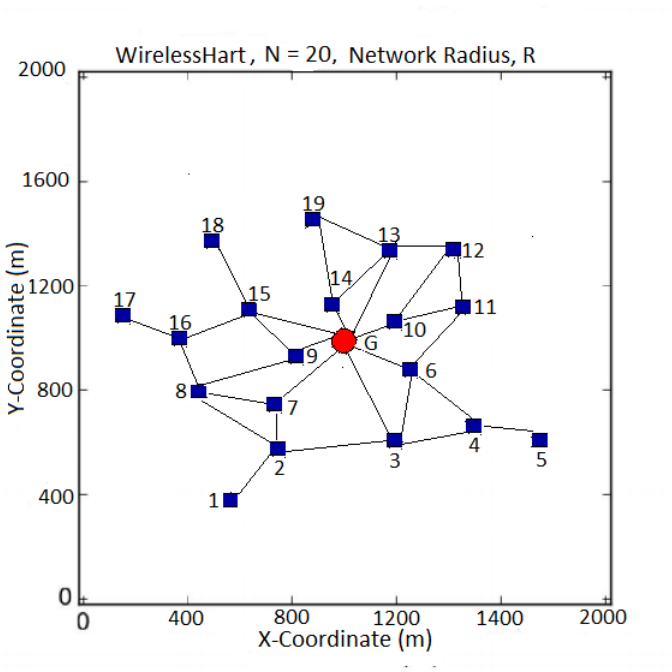


Figure 5.15: 20 Node Random Test Topology for WirelessHart Protocol

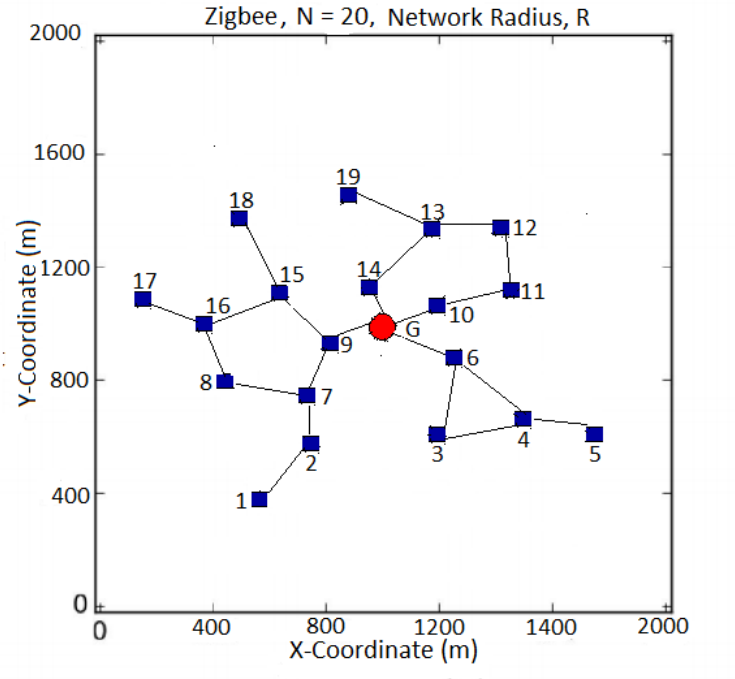


Figure 5.16: 20 Node Random Test Topology for Zigbee Protocol

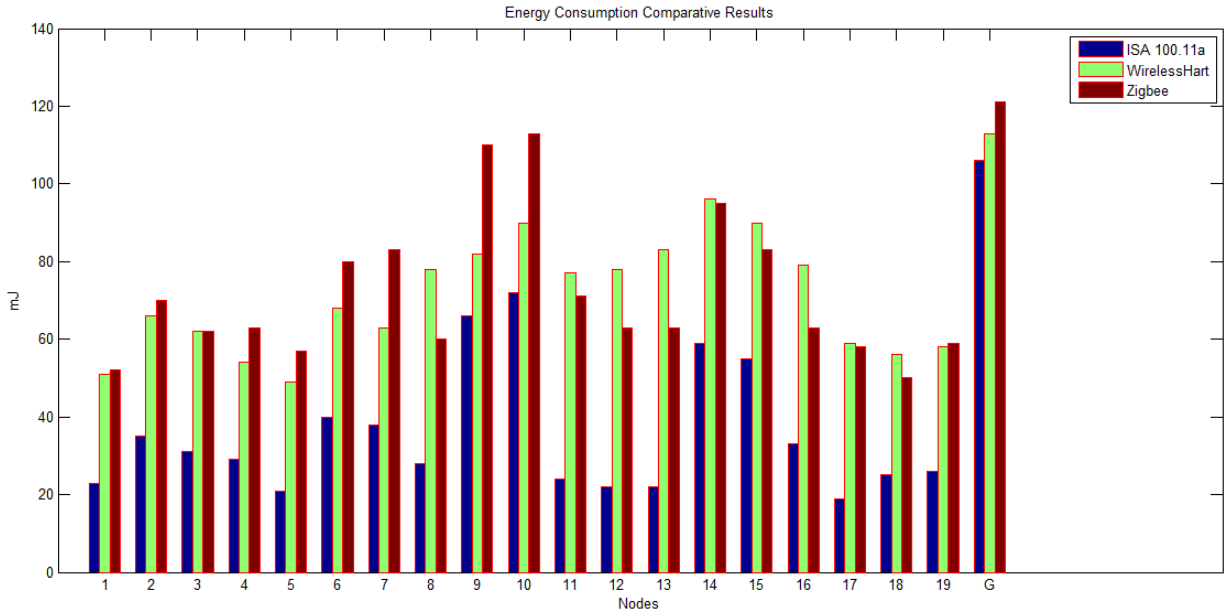


Figure 5.17: Performance Comparison - Energy Consumption

This pattern is observed for all network nodes except nodes 11 to 18 where most of these nodes act as relays, WirelessHart consumes more than Zigbee. It is also observed that nodes closest to the base station like 9, 10, 14 and 15 consumed more as compared to those furthest from the base station due to the fact that most of these node act as relays with nodes 1, 17, 18 and 19 consuming the least energy since they are seldom used to relay packets from other node in all three protocols. This is expected since, nodes closest to the base station although have a shorter transmission and reception times as compared to those furthest from the base station mostly act as relays and hence transmit and receive more packets and also goes through a lot of processing. Hence we observe nearly the same consumption pattern for nodes for the same topology but ISA 100.11a consumes less on average than the other protocols and Zigbee consumes most on average.

5.3.4.2 Received Packet Statistics Comparison

Figure 5.18 shows the packet loss per node of each network node for Zigbee, WirelessHart and ISA 100.11a protocols. It is observed that the number of packet lost by all nodes fall within a range of 27 and 221 for all three protocols. As shown in Figure 5.18 the base station node incurred the most lost packets which is expected since the base station communicates with all network nodes. As shown in Figure 5.18, for nodes closest to the base station, like 9, 10, 14 and 15, Zigbee incurs a higher number of packet loss as compared to WirelessHart and ISA 100.11a and the same pattern is observed for nodes furthest from the base station like node 1, 5, 11, 12, 13, 17, 18 and 19 but at a much higher intensity due to collisions and interferences. Hence WirelessHart can be said to out performs Zigbee in longer transmission ranges and vise versa but ISA 100.11a outperforms all the other protocols in terms of successful transmissions.

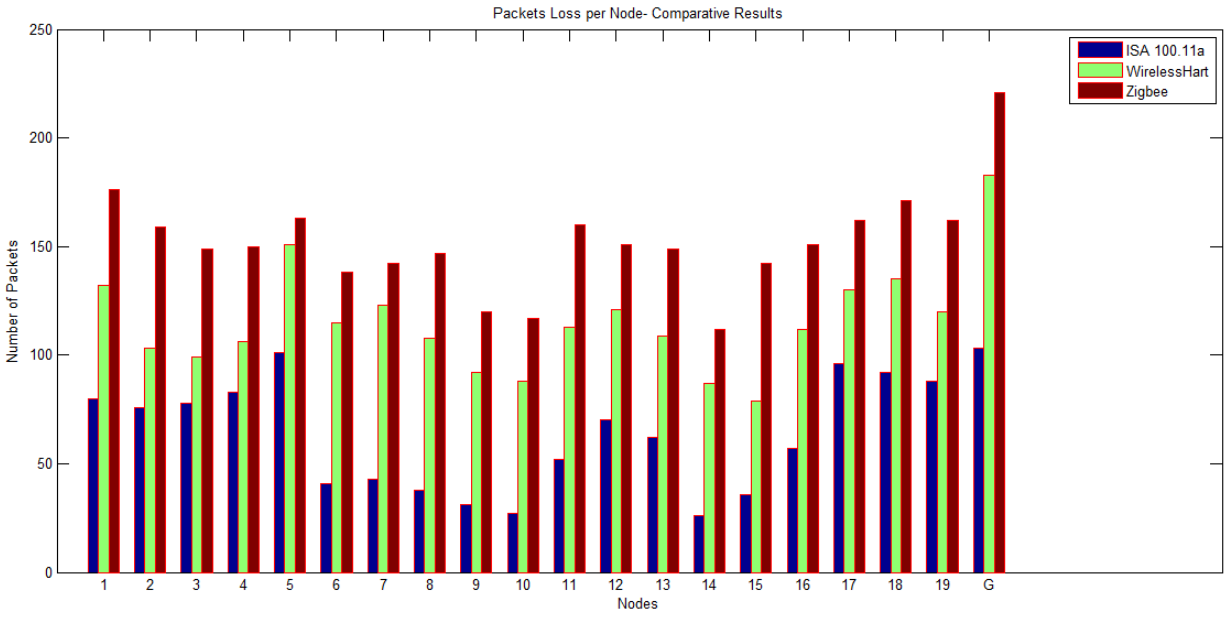


Figure 5.18: Comparison: Received Packet Statistics

The number of lost packets at the base station for WirelessHart was 38 less than

Zigbee whereas the base station packet loss for ISA 100.11a is observed to be the least. On average, Zigbee registered the most loss in packets, with an average of 134.8 as compared to that of 110.3 for WirelessHart and 60.0 for ISA 100.11a. Hence, in their respective transmission ranges, the accuracy of Zigbee on average is higher than that of WirelessHart but ISA 100.11a has the least accuracy among the three protocols.

CHAPTER 6

CONCLUSION

In this work, we presented the significance of Industrial Wireless Sensor Networks (IWSNs) in industrial automation. Industrial wireless sensor networks face a lot of challenges in their implementation and operation. We then reviewed of three commonly employed WSN protocols in industrial environment and survey of existing WSN-based industrial solutions. We also provided background of diversity techniques and channel fading.

The broadcast nature of the wireless channel can be exploited to enhance system diversity by processing multiple copies of the same signal, however it resulted into an interference-limited system, degrading the system performance. We proposed two configurations for IWSN, where the first configuration strives to enhance the reliability of the system while the second aspires to enhance the spectral efficiency, using the two metrics, i.e., bit error rate (BER) and outage probability for the performance analysis of the proposed configurations.

In this work, we have studied and conducted the lab test of Zigbee, Wireless HART

and ISA 100.11a. The results were compared and analyzed in order to evaluate the best protocol for IWSNs. The Yokogawa field wireless kit offers a far better range that is greater than 800 meters, which is suitable for bigger industries and cuts the cost of additional gateway devices used to connect all the edges in a factory. Results obtained from these practical experiments we compared to simulation results under similar network conditions.

Finally, we have studied and conducted the simulation of Zigbee, Wireless HART and ISA100. The topologies were generated using the Pymote framework. The protocols performance were simulated using pymote. The simulation results are analyzed using plots and charts. The results were compared and analyzed in order to evaluate the best protocol for IWSNs. ISA 100.11a was observed to present the best performance in terms of Packet error rate and energy consumption as compared to WirelessHart and Zigbee.

6.1 Contributions

- A survey of the existing technologies and protocols related to industrial wireless sensor networks.
- A study on the feasibility and challenges of utilizing wireless sensor networks for industrial applications.
- The development of a combining technique for relay-based cooperative wireless sensor networks.
- An experimental and simulation performance evaluation of wireless sensor networks

in industrial environments.

6.2 Future Work

Future research could incorporate an comprehensive mathematical analysis of the performance on Zigbee, WirelessHart and ISA 100.11a. Also, a more thorough evaluation of the error correction technique on different network scenarios could be carried out in future research. Moreover, a more robust combining technique for co-operative IWSNs could be developed based on our proposed scheme. Finally, a Medium Access Control (MAC) performance evaluation for Zigbee, WirelessHart and ISA-100.11a protocols could be researched.

6.3 Publications

[1] Al-Yami, A.M.; Harb, K. and Abduljauwad, S., "Industrial Wireless Sensor Networks in the perspective of diversity and spectral efficiency," in Communications (MICC), 2013 IEEE Malaysia International Conference on , vol., no., pp.390-395, 26-28 Nov. 2013, doi: 10.1109/MICC.2013.6805860

[2] Al-Yami, A. and Abu-Al-Saud, W.,"Practical vs. Simulated Results of ISA100 Physical Layer," in Intelligent Systems, Modelling and Simulation (ISMS), 2015 6th International Conference on , vol., no., pp.226-230, 9-12 Feb. 2015, doi: 10.1109/ISMS.2015.47

[3] Al-Yami, A. and Abu-Al-Saud, W., Industrial Wireless Sensor Networks (ISWN): Requirements and Solutions, Proc. of SPACOMM, Lisbon, Portugal, 2016

[4] Al-Yami, A.; Abu-Al-Saud, W., and Shahzad, F., Simulation of Industrial Wireless Sensor Network (IWSN) Protocols, 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS): 2016 IEEE Infocom MiseNet Workshop), pp., 10-14 April 2016, doi: 10.1109/INFCOMW.2016.7562133

[5] Al-Yami, A.; Abu-Al-Saud, W. and Shahzad, F., On Industrial Wireless Sensor Network (IWSN) and its Simulation using Castalia, 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation, pp .293-298, May, 2016, doi:10.1109/UKSim.2016.5

REFERENCES

[1] Y.-c. T. Meng-shiuan Pan, "Communication Protocols and Applications for ZigBee-Based Wireless Sensor Networks." [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.320.5360

[2] A. M. Al-Yami, K. Harb, and S. Abduljauwad, "Industrial Wireless Sensor Networks in the perspective of diversity and spectral efficiency," in *2013 IEEE 11th Malaysia International Conference on Communications (MICC)*. IEEE, nov 2013, pp. 390–395. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6805860

[3] A. Al-Yami and W. Abu-Al-Saud, "Practical vs. Simulated Results of ISA100 Physical Layer," in *2015 6th International Conference on Intelligent Systems, Modelling and Simulation*. IEEE, feb 2015, pp. 226–230. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7311242

[4] A. Willig, K. Matheus, and A. Wolisz, "Wireless Technology in Industrial Networks," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1130–1151, jun 2005. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1435743

[5] J. Song, S. Han, A. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt, "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control," in *2008 IEEE Real-Time and Embedded Technology and Applications Symposium*. IEEE, apr 2008, pp. 377–386. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4550808

[6] P. Ferrari, A. Flammini, S. Rinaldi, and E. Sisinni, "Performance assessment of a WirelessHART network in a real-world testbed," in *2012 IEEE International Instrumentation and Measurement Technology Conference Proceedings*. IEEE, may 2012, pp. 953–957. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6229177

[7] S. Petersen, P. Doyle, S. Vatland, C. S. Aasland, T. M. Andersen, and D. Sjong, "Requirements, drivers and analysis of wireless sensor network solutions for the Oil Gas industry," in *Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on*, sep 2007, pp. 219–226.

[8] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, "Comparison of industrial WSN standards," *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on*, 2010.

[9] M. K. Simon and M.-S. Alouini, *Digital communication over fading channels*. John Wiley & Sons, 2005, vol. 95.

[10] G. L. Stüber, *Principles of Mobile Communication (2Nd Ed.)*. Norwell, MA, USA: Kluwer Academic Publishers, 2001.

[11] A. M. Al-Yami, K. Harb, and S. Abduljauwad, "Industrial wireless sensor networks in the perspective of diversity and spectral efficiency," in *Communications (MICC), 2013 IEEE Malaysia International Conference on.* IEEE, 2013, pp. 390–395.

[12] H. Q. Huynh, J. Yuan, and H. Suzuki, "Performance analysis for a multi-branch nonregenrative relay system with mrc in nakagami-m channels," in *Signal Processing Advances in Wireless Communications, 2008. SPAWC 2008. IEEE 9th Workshop on.* IEEE, 2008, pp. 575–579.

[13] N. C. Beaulieu and A. A. Abu-Dayya, "Analysis of equal gain diversity on nakagami fading channels," *IEEE Transactions on Communications*, vol. 39, no. 2, pp. 225–234, 1991.

[14] W. Al-Yami, A.; Abu-Al-Saud and F. Shahzad, "Simulation of industrial wireless sensor network (iwsn) protocols," I. C. on Computer Communications Workshops (INFOCOM WKSHPS):, Ed., IEEE. IEEE, apr 2016, pp. 10–14.

[15] A. Al-Yami and W. Abu-Al-Saud, "Industrial wireless sensor networks (iswn): Requirements and solutions," P. Proc. of SPACOMM, Lisbon, Ed., 2016.

[16] A. Abuarqoub, F. Alfayez, M. Hammoudeh, T. Alsboui, and A. Nisbet, "Simulation Issues in Wireless Sensor Networks: A Survey," in *SENSORCOMM 2012 , The Sixth International Conference on Sensor Technologies and Applications*, aug 2012, pp. 222–228.

[17] Q. Ali, A. Abdulmaowjod, and H. Mohammed, "Simulation & performance study of wireless sensor network (WSN) using MATLAB," in *Power and Control (EPC-IQ), 1st International Conference on*, 2010, pp. 307–314.

[18] Y. Tselishchev, A. Boulis, and L. Libman, "Experiences and Lessons from Implementing a Wireless Sensor Network MAC Protocol in the Castalia Simulator," in *2010 IEEE Wireless Communication and Networking Conference*. IEEE, apr 2010, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5506096

[19] L. Shu, M. Hauswirth, H.-C. Chao, M. Chen, and Y. Zhang, "NetTopo: A framework of simulation and visualization for wireless sensor networks," *Ad Hoc Networks*, vol. 9, no. 5, pp. 799–820, jul 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870510001435

[20] A. Kroeller, D. Pfisterer, C. Buschmann, S. P. Fekete, and S. Fischer, "Shawn: A new approach to simulating wireless sensor networks," p. 10, feb 2005. [Online]. Available: http://arxiv.org/abs/cs/0502003

[21] F. J. &. A. Marculescu, "AlgoSenSim - Overview [TCS-Sensor Lab]," 2006. [Online]. Available: http://tcs.unige.ch/doku.php/code/algosensim/overview

[22] "Sinalgo." [Online]. Available: http://dcg.ethz.ch/projects/sinalgo/

[23] A. Sobeih, "J-Sim: A Simulation and emulation environment for wireless sensor networks," *IEEE Wireless Communications*, vol. 13, no. 4, pp. 104–119, aug

2006. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1678171

[24] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems*, pp. 60:1—-60:10, mar 2008. [Online]. Available: http://dl.acm.org/citation.cfm?id=1416222.1416290

[25] A. Boulis, "Castalia - Wireless Sensor Network Simulator," 2011. [Online]. Available: https://castalia.forge.nicta.com.au/index.php/en/index.html

[26] D. Arbula and K. Lenac, "Pymote: High Level Python Library for Event-Based Simulation and Evaluation of Distributed Algorithms," *International Journal of Distributed Sensor Networks*, vol. 2013, no. 797354, p. 12, 2013.

[27] F. Shahzad, "Extending the Functionality of Pymote: Low Level Protocols and Simulation Result Analysis," *International Journal of Sensor Networks and Data Communications*, vol. 04, no. 02, nov 2015.

[28] F. Shahzad and T. R. Sheltami, "An efficient MAC scheme in wireless sensor network with energy harvesting (EHWSN) for cloud based applications," in *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*. IEEE, oct 2015, pp. 783–788. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7365928

[29] J. D. Hunter, "Matplotlib: A 2D Graphics Environment," *Computing in Science & Engineering*, vol. 9, no. 3, pp. 90–95, 2007. [Online]. Available: http://scitation.aip.org/content/aip/journal/cise/9/3/10.1109/MCSE.2007.55

[30] T. Høns, "Highcharts, Highstock and Highmaps documentation — Highcharts," 2013. [Online]. Available: http://www.highcharts.com/docs

[31] W. Al-Yami, A.; Abu-Al-Saud and F. Shahzad, "On industrial wireless sensor network (iwsn) and its simulation using castalia," . . U.-A. 18th International Conference on Computer Modelling and M. .-d. Simulation, Eds., no. 293-298, UKSim-AMSS. UKSim-AMSS 18th International Conference on Computer Modelling and Simulation, may 2016.

Vitae

- **Name**: Abdullah M. Al-Yami
- **Nationality**: Saudi
- **Date of Birth**: 19^{th} April, 1988
- **Email**: *abdullah.yami.22@aramco.com*
- **Permanent Address**: Box 18576, Dhahran City 31311, KSA

Academic Background

- Masters Degree in Science of Electrical Engineering at KFUPM, Dhahran, KSA in January 2017.
- Bachelors Degree in Science of Electrical Engineering at KFUPM, Dhahran, KSA from August 2012.